#2 Priority Paper

Docket No. 826.1547/JDH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
Yasutsugu KURODA, et al.	Group Art Unit: To Be Assigned
Serial No.: To Be Assigned	
Filed: June 8, 1999	Examiner: To Be Assigned
For: ELECTRONIC DATA STORAGE APPARATUS WITH KEY MANAGEMENT FUNCTION AND ELECTRONIC DATA STORAGE METHOD	

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, Applicants submit herewith a certified copy of each of the following foreign application:

Japanese Appln. No. 10-360345, filed December 18, 1998.

It is respectfully requested that Applicants be given the benefit of the earlier foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY

Dated: June 8, 1999 By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: December 18, 1998

Application Number: Patent Application No. 10-360345

Applicant(s): FUJITSU LIMITED

March 12, 1999

Commissioner,
Patent Office Takeshi ISAYAMA

Certificate No.11-3014881

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed this Office.

願 年 月 日
Date of Application: １９９８年１２月１８日

願 番 号
Application Number: 平成１０年特許願第３６０３４５号

願 人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年 ３月１２日

特 許 庁 長 官
Commissioner,
Patent Office 伊佐山建志

【書類名】　特許願

【整理番号】　9804916

【提出日】　平成10年12月18日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/08

G09C　1/00

【発明の名称】　鍵管理機能付電子データ保管装置および電子データ保管方法

【請求項の数】　21

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　黒田　　康嗣

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　蒲田　順

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　岩瀬　　詔子

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　野田　敏達

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小野　越夫

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100074099

【郵便番号】　102

【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ

【弁理士】

【氏名又は名称】　大菅　義之

【電話番号】　03-3238-0031

【選任した代理人】

【識別番号】　100067987

【郵便番号】　222

【住所又は居所】　神奈川県横浜市港北区太尾町１４１８－３０５（大倉山二番館）

【弁理士】

【氏名又は名称】　久木元　彰

【電話番号】　045-545-9280

【手数料の表示】

【予納台帳番号】　012542

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705047

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　鍵管理機能付電子データ保管装置および電子データ保管方法

【特許請求の範囲】

【請求項１】　電子データを保管する電子データ保管装置において、

自電子データ保管装置に固有の個別鍵と、他の電子データ保管装置との間で共通の共通鍵とを管理する鍵管理手段と、

自電子データ保管装置内に保管する電子データに対しては前記個別鍵を用いて暗号処理を行い、他電子データ保管装置との間で送信、または受信する電子データに対しては、前記共通鍵を用いて暗号処理、またはデータ検証を行う暗号処理手段とを備えることを特徴とする鍵管理機能付電子データ保管装置。

【請求項２】　前記鍵管理手段が、前記共通鍵として複数の電子データ保管装置によって構成される１つのグループ内で共通のグループ鍵を管理することを特徴とする請求項１記載の鍵管理機付電子データ保管装置。

【請求項３】　前記１つのグループ内に主となる電子データ保管装置が存在し、

該主となる電子データ保管装置の前記暗号処理手段が、自装置の個別鍵を用いて該１つのグループ内の個々の電子データ保管装置の個別鍵を生成し、

該生成された個別鍵が該１つのグループに属する個々の電子データ保管装置に配布されることを特徴とする請求項２記載の鍵管理機能付電子データ保管装置。

【請求項４】　前記１つのグループ内に主となる電子データ保管装置が存在し、

該主となる電子データ保管装置の前記暗号処理手段が、自装置の個別鍵を用いて前記１つのグループ内で共通のグループ鍵を生成し、

該生成されたグループ鍵が該１つのグループに属する個々の電子データ保管装置に配布されることを特徴とする請求項２記載の鍵管理機能付電子データ保管装置。

【請求項５】　前記１つのグループ内に主となる電子データ保管装置が存在し、

該主となる電子データ保管装置の前記暗号処理手段が、前記個別鍵として該主

となる電子データ保管装置の使用開始前にあらかじめ割り当てられている鍵と、新たに外部から指定される鍵とを関連づけて前記１つのグループ内で共通のグループ鍵を生成し、

該生成されたグループ鍵が該１つのグループに属する個々の電子データ保管装置に配布されることを特徴とする請求項２記載の鍵管理機能付電子データ保管装置。

【請求項６】　前記１つのグループ内に主となる電子データ保管装置が存在すると共に、該複数のグループ内の該主となる電子データ保管装置のそれぞれを管理するグループ管理用電子データ保管装置が存在し、

該グループ管理用電子データ保管装置の前記暗号処理手段が、自装置の個別鍵を用いて該主となる電子データ保管装置のそれぞれの個別鍵を生成し、

該生成された個別鍵が該主となる電子データ保管装置のそれぞれに配布されることを特徴とする請求項２記載の鍵管理機能付電子データ保管装置。

【請求項７】　前記鍵管理手段が前記共通鍵として、前記グループ鍵に加えて、自電子データ保管装置が属するグループと異なるグループに属する電子データ保管装置との間での電子データの送受信に用いられる公開鍵を管理することを特徴とする請求項２記載の鍵管理機能付電子データ保管装置。

【請求項８】　前記個別鍵が前記電子データ保管装置の使用開始前にあらかじめ各電子データ保管装置に割り当てられていることを特徴とする請求項１記載の鍵管理機能付電子データ保管装置。

【請求項９】　前記暗号処理手段が、自電子データ保管装置の使用開始前にあらかじめ設定されている鍵と、外部から新たに指定される鍵とを関連づけて前記個別鍵を生成し、

前記鍵管理手段が該生成された個別鍵を管理することを特徴とする請求項１記載の鍵管理機能付電子データ保管装置。

【請求項１０】　前記鍵管理手段が、前記個別鍵と共通鍵とに加えて、全ての電子データ保管装置に共通のマスタ鍵を管理することを特徴とする請求項１記載の鍵管理機能付電子データ保管装置。

【請求項１１】　前記暗号処理手段が、前記マスタ鍵を用いて自電子データ

保管装置を識別する情報を暗号化して、前記個別鍵を生成し、

前記鍵管理手段が該生成された個別鍵を管理することを特徴とする請求項１０記載の鍵管理機能付電子データ保管装置。

【請求項１２】　複数の電子データ保管装置によって構成される１つのグループ内に主となる電子データ保管装置が存在し、

該主となる電子データ保管装置の前記暗号処理手段が、前記生成された個別鍵を用いて前記１つのグループを識別する情報を暗号化して前記共通鍵としてのグループ鍵を生成し、

該生成されたグループ鍵が該１つのグループに属する個々の電子データ保管装置に配布されることを特徴とする請求項１１記載の鍵管理機能付電子データ保管装置。

【請求項１３】　それぞれ複数の電子データ保管装置によって構成されるグループを１つの階層とする電子データ保管装置の階層構造が構成され、

前記鍵管理手段が、自装置が属するグループの階層に応じたグループ鍵を前記共通鍵として管理することを特徴とする請求項１記載の鍵管理機能付電子データ保管装置。

【請求項１４】　前記電子データ保管装置の階層構造において、上位側の階層のグループ内に直近下位の階層のグループの電子データ保管装置を管理する管理用電子データ保管装置が存在し、

該管理用電子データ保管装置の前記暗号処理手段が、自装置の個別鍵を用いて該下位階層に対応するグループ鍵を生成し、

該生成されたグループ鍵が該直近下位の階層のグループの電子データ保管装置に配布されることを特徴とする請求項１３記載の鍵管理機能付電子データ保管装置。

【請求項１５】　それぞれ複数の電子データ保管装置によって構成されるグループを１つの階層とする階層構造内の電子データ保管装置における電子データ保管方法であって、

該階層構造の１つの階層内の送信側電子データ保管装置が、自装置内に保管され、自装置に固有の個別鍵を用いて暗号処理されているデータを、該１つの階層

に対応する上位グループ鍵によって暗号処理し直して、該階層構造で直近下位の階層の電子データ保管装置を管理する下位グループ管理用電子データ保管装置に送信し、

該下位グループ管理用電子データ保管装置が前記上位グループ鍵を用いて受信したデータを検証し、

該検証の結果、電子データが正しければ前記直近下位の階層に対応する下位グループ鍵によって該電子データを暗号処理し直して該直近下位階層内の受信側電子データ保管装置に送信し、

該受信側電子データ保管装置が該下位グループ鍵を用いて受信データを検証し、

該検証の結果、電子データが正しければ、自装置に固有の個別鍵を用いて受信データを暗号処理し直して保管することを特徴とする電子データ保管方法。

【請求項１６】　それぞれ複数の電子データ保管装置によって構成されるグループを１つの階層とする階層構造内の電子データ保管装置における電子データ保管方法であって、

該階層構造の１つの階層内の送信側電子データ保管装置が、自装置内に保管され、自装置に固有の個別鍵を用いて暗号処理されているデータを、該１つの階層に対応する下位グループ鍵によって暗号処理し直して、該１つの階層の電子データ保管装置を管理する下位グループ管理用電子データ保管装置に送信し、

該下位グループ管理用電子データ保管装置が前記下位グループ鍵を用いて受信したデータを検証し、

該検証の結果、電子データが正しければ前記１つの階層の直近上位の階層に対応する上位グループ鍵によって該電子データを暗号処理し直して該直近上位階層内の受信側電子データ保管装置に送信し、

該受信側電子データ保管装置が該上位グループ鍵を用いて受信データを検証し、

該検証の結果、電子データが正しければ、自装置に固有の個別鍵を用いて受信データを暗号処理し直して保管することを特徴とする電子データ保管方法。

【請求項１７】　電子データを保管する電子データ保管装置における電子デ

ータ保管方法であって、

他の電子データ保管装置との間で共通の共通鍵を用いて電子データの通信を行い、

自電子データ保管装置に保管すべきデータに対しては自電子データ保管装置に固有の個別鍵を用いて暗号処理を行うことを特徴とする電子データ保管方法。

【請求項１８】　前記電子データ保管装置が、前記共通鍵として複数の電子データ保管装置によって構成される１つのグループ内で共通のグループ鍵を保存し、

送信側の電子データ保管装置が、自電子データ保管装置内に保管され、前記個別鍵を用いて暗号処理されている電子データを該グループ鍵によって暗号処理し直して、該電子データを送信し、

受信側の電子データ保管装置が受信した電子データを該グループ鍵を用いて検証し、

検証の結果、電子データが正しければ、該電子データを前記個別鍵を用いて暗号処理し直して保管することを特徴とする請求項１７記載の電子データ保管方法。

【請求項１９】　前記電子データ保管装置が前記共通鍵として、複数の電子データ保管装置によって構成され、自電子データ保管装置が属する１つのグループと異なる他のグループに属する電子データ保管装置の公開鍵を保存し、

送信側の電子データ保管装置が、自電子データ保管装置内に保管され、前記個別鍵を用いて暗号処理されている電子データを該公開鍵によって暗号処理し直して、該電子データを送信し、

受信側の電子データ保管装置が受信した電子データを該公開鍵と対となる秘密鍵を用いて検証し、

検証の結果、電子データが正しければ、該電子データを前記個別鍵を用いて暗号処理し直して保管することを特徴とする請求項１７記載の電子データ保管方法。

【請求項２０】　電子データ保管装置において使用される記憶媒体であって、

保管されている電子データを自装置に固有の個別鍵を用いて検証させる機能と、

該検証の結果が正しければ、該電子データを該電子データ受信側と共通の共通鍵を用いて暗号処理し直して受信側に送信させる機能とを備えるプログラムを格納した計算機読み出し可能記憶媒体。

【請求項２１】　電子データ保管装置において使用される記憶媒体であって、

外部から受信した電子データを該電子データ送信側と共通の共通鍵を用いて検証させる機能と、

該検証の結果が正しければ該電子データを自装置に固有の個別鍵を用いて暗号処理し直して保管させる機能とを備えるプログラムを格納した計算機読み出し可能記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は電子文書の安全性に係り、更に詳しくはローカルな環境とグローバルな環境とにおいて、文書としての電子データの暗号処理に用いる鍵を変えることによって、電子データの安全性を確保する鍵管理機能付電子データ保管装置、および電子データ保管方法に関する。

【０００２】

【従来の技術】

企業間における電子商取引などの進展、公共分野の電子化等に伴い、契約書や戸籍謄本などの重要文書の電子化、ネットワーク化が本格化しようとしている。

【０００３】

一般の契約や更新手続きでは、書類の原本（契約書、申請書、領収書等）と、その写し（謄本、抄本等）が必要になることがよくある。紙媒体では原本と写しは明確に区別ができる。これは原本と写しとでは、用紙やインクの物理的な性質が異なるためである。同様の理由で原本の改ざんも困難であった。

【０００４】

しかし電子文書は一般に簡単に複製を行うことができ、２つの電子文書が同じ内容を持ちながら存在することになるため、どちらが本物の原本か分からなくなるなどの問題がおこる。そのため一旦電子化処理された重要文書をわざわざ紙に印刷して保管したり、郵送したりしなければならないというような事態も存在した。

【０００５】

また重要文書を電子文書のままで保管したり移動したりする場合には、従来は電子データの保管装置に共通なアルゴリズムを用いて、文書を構成する電子データに対する暗号処理を行って安全性を確保するという方法がとられている。このアルゴリズムに用いられる鍵の種類は大きく２つに区別することができる。一方は電子データの送信者と受信者で共通な鍵を用いる慣用暗号であり、もう一方は公開鍵と秘密鍵の対を用いる公開鍵暗号である。

【０００６】

【発明が解決しようとする課題】

このように従来においては、例えば同一種類の電子データを保管する電子データ保管装置相互間、すなわちローカルな環境と、異なる種類の電子データを保管し、不特定多数の電子データ保管装置相互間で通信を行うグローバルな環境とでは、暗号処理に使用される鍵を変えることによって電子文書の安全性を確保していたが、電子データ保管装置において共通なアルゴリズムを用いているために、グローバルな環境でも電子データ保管装置に共通な鍵を用いてしまったり、ローカルな環境でも公開鍵を用いてしまうような運用が行われることがあった。

【０００７】

このためローカルな環境のみにおいて使用される電子データ保管装置に対しても公開鍵の運用に必要な認証局を運営してしまったり、グローバルな環境において電子データ保管装置に共通な鍵が暴露してしまうことによって全ての重要文書の信頼性が失われてしまうという問題があった。

【０００８】

本発明の目的は、電子データ保管装置に電子データを保管する時にはその保管装置に固有の個別鍵を用いて電子データに対する暗号処理を行い、他の電子デー

タ保管装置との間で電子データの送受信を行う場合にはローカルな環境、またはグローバルな環境にそれぞれ適合した共通鍵を用いて暗号処理を行って電子データの送受信を行うことによって、それぞれの環境にあった鍵管理を実現できる鍵管理機能付電子データ保管装置を提供することである。

【０００９】

本発明の他の目的は、個別鍵を用いて暗号処理されている電子データを共通鍵で暗号化処理し直して、他の電子データ保管装置との間で電子データの送受信を行うことにより、電子データの安全性を確保することができる電子データ保管方法を提供することである。

【００１０】

【課題を解決するための手段】

図１は本発明の原理構成ブロック図である。同図は電子データを保管する時には自装置に固有の個別鍵を用いて電子データを暗号処理して保管し、他の電子データ保管装置との間でデータ送受信を行う時にはローカルな環境、またはグローバルな環境にそれぞれ適合した共通鍵を用いてデータ送受信を行う鍵管理機能付電子データ保管装置１の原理構成ブロック図である。

【００１１】

図１において、鍵管理手段２は自装置に固有の個別鍵と、他の電子データ保管装置との間で共通の共通鍵とを管理するものであり、例えば鍵管理部である。

【００１２】

暗号処理手段３は、自装置内に保管する電子データに対しては個別鍵を用いて暗号処理を行い、他の電子データ保管装置との間で送受信する電子データに対しては共通鍵を用いた暗号処理、またはデータ検証を行うものであり、例えば暗号処理部である。

【００１３】

本発明の実施の形態においては、鍵管理手段２によって管理される共通鍵は、複数の電子データ保管装置によって構成される１つのグループ内で共通のグループ鍵とすることも可能である。

【００１４】

この時、１つのグループ内に主となる電子データ保管装置が存在し、その保管装置の暗号処理手段３が、自装置の個別鍵を用いてその 1つのグループ内の個々の電子データ保管装置の個別鍵を生成し、その生成された個別鍵が個々の電子データ保管装置に配布されることも、また同様にグループ鍵が生成されて配布されることも可能であり、グループ鍵が主となる電子データ保管装置にあらかじめ割り当てられている鍵と、新たに外部から指定される鍵とが関連づけられて生成されて、配布されることも可能である。

【００１５】

さらに複数のグループ内の主となる電子データ保管装置のそれぞれを管理するグループ管理用電子データ保管装置が存在し、その保管装置の暗号処理手段３が、自装置の個別鍵を用いて主となる電子データ保管装置のそれぞれの個別鍵を生成して、生成された個別鍵が主となる電子データ保管装置に配布されることも可能である。

【００１６】

次に鍵管理手段２は、グループ鍵に加えて、自装置が属するグループと異なるグループに属する電子データ保管装置との間でのデータ送受信に用いるための公開鍵を、通信用の鍵として管理することもできる。

【００１７】

本発明の実施の形態においては、鍵管理手段２が個別鍵と共通鍵とに加えて、全ての電子データ保管装置に共通のマスタ鍵を管理することもできる。

【００１８】

この時各電子データ保管装置の暗号処理手段３は、このマスタ鍵を用いて自装置を識別する情報を暗号化して個別鍵を生成することもでき、また１つのグループ内に主となる電子データ保管装置が存在する場合には、その保管装置の暗号処理手段３が自装置内で生成した個別鍵を用いてそのグループを識別する情報を暗号化してグループ鍵を生成し、生成されたグループ鍵がそのグループに属する個々の電子データ保管装置に配布されることも可能である。

【００１９】

さらに本発明の実施の形態においては、それぞれ複数の電子データ保管装置に

よって構成されるグループを１つの階層とする階層構造が構成され、鍵管理手段２が自装置が属するグループの階層に応じたグループ鍵を共通鍵として管理することもでき、またこの階層構造において上位側の階層のグループ内に、直近下位の階層のグループの電子データ保管装置を管理する管理用電子データ保管装置が存在し、その管理用電子データ保管装置が自装置の個別鍵を用いて直近下位の階層に対応するグループ鍵を生成し、生成されたグループ鍵が直近下位の階層の電子データ保管装置に配布されるようにすることも可能である。

【００２０】

次に本発明の電子データ保管方法においては、他の電子データ保管装置との間で共通の共通鍵を用いて電子データの通信が行われ、自装置に保管すべきデータに対しては、自装置に固有の個別鍵を用いて暗号処理が行われる。

【００２１】

本発明の実施の形態としての電子データ保管方法においては、共通鍵として複数の電子データ保管装置によって構成される１つのグループ内で共通のグループ鍵が保持され、送信側の電子データ保管装置内でその装置固有の個別鍵を用いて暗号処理されている電子データが、グループ鍵によって暗号処理し直されて送信され、受信側の電子データ保管装置によって受信された電子データがグループ鍵を用いて検証され、検証の結果電子データが正しければ、その電子データが受信側の装置に固有の個別鍵を用いて暗号処理し直して保管されることもできる。

【００２２】

また、本発明の実施の形態としての電子データ保管方法においては、共通鍵として自装置が属するグループと異なる他のグループに属する電子データ保管装置の公開鍵が保持され、送信側の装置が自装置内に保持され、個別鍵を用いて暗号処理されている電子データを公開鍵によって暗号処理し直して送信し、受信側の装置が受信した電子データを公開鍵と対となる秘密鍵を用いて検証し、検証の結果が正しければ、その電子データを受信側の電子データ保管装置に固有の個別鍵を用いて暗号処理し直して保管するようにすることも可能である。

【００２３】

また本発明の電子データ保管装置において使用される記憶媒体として、保管さ

れている電子データを自装置に固有の個別鍵を用いて検証させる機能と、検証の結果が正しければ、その電子データを受信側と共通の共通鍵を用いて暗号処理し直して送信させる機能とを備えるプログラムを格納した計算機読み出し可能記憶媒体を用いることもできる。

【００２４】

また電子データ保管装置において使用される記憶媒体として、外部から受信した電子データを送信側と共通の共通鍵を用いて検証させる機能と、その検証の結果が正しければ、その電子データを自装置に固有の個別鍵を用いて暗号処理し直して保管させる機能とを備えるプログラムを格納した計算機読み出し可能記憶媒体を用いることもできる。

【００２５】

以上のように本発明によれば、自装置に保管すべき電子データに対しては自装置に固有の個別鍵を用いて暗号処理を行い、また他の電子データ保管装置との間で送受信する電子データに対しては、相手側の装置との間で共通の共通鍵を用いて電子データの暗号処理と、その検証が行われる。

【００２６】

【発明の実施の形態】

図２は本発明の第１の実施形態における鍵管理機能付電子データ保管装置の構成ブロック図である。本発明の第１の実施形態においては、電子データ保管装置１０の内部には個別鍵、グループ鍵、および公開鍵の３種類の鍵が保持される。

【００２７】

図２において制御部１１は全体の動作を制御するものである。鍵管理部１２は電子データ保管装置１０の内部に保持されている鍵を管理するものであり、暗号処理部１３は必要に応じて鍵を生成したり、電子データを暗号化したり、電子データを検証する処理を行うものである。

【００２８】

個別鍵保持部１４はその電子データ保管装置１０に固有の個別鍵を保持し、グループ鍵保持部１５は複数の電子データ保管装置１０によって構成される１つのグループ内での共通鍵としてのグループ鍵を保持するものであり、公開鍵保持部

１６は、例えば他のグループに属する電子データ保管装置１０との間で電子データの送受信を行う場合に使用される公開鍵を保持するものである。

【００２９】

電子データ保管装置１０の内部には、更に電子データを保管するデータ保管部１７と、他の電子データ保管装置との間で電子データの送受信を行うための通信処理部１８が備えられている。通信処理部１８はネットワークとして接続されている。

【００３０】

図３は本発明の第１の実施形態における電子データ保管装置の全体処理フローチャートである。同図において、ステップＳ１で電子データが入力されるか、または例えば電子データの送信指示が入力されると、ステップＳ２で電子データ保管装置へのデータ保存か否かが判定される。なおステップＳ１での送信指示は保管装置の利用者、またはアプリケーションから、例えばネットワークを介して与えられる。

【００３１】

データの保存である場合には、ステップＳ３で鍵管理部１２によって個別鍵保持部１４が保持する個別鍵が選択され、ステップＳ４で個別鍵を用いて暗号処理部１３によって電子データに対する暗号処理が行われ、ステップＳ５でデータ保管部１７にデータが保管されて処理を終了する。

【００３２】

ステップＳ２でデータの保存でない場合には、ステップＳ６で、ステップＳ１で与えられた指示がグループ内の電子データ保管装置との間でのデータの送受信か否かが判定され、グループ内のデータ送受信である場合には、ステップＳ７で鍵管理部１２によってグループ鍵保持部１５が保持するグループ鍵が選択され、ステップＳ８で暗号処理部１３によってグループ鍵を用いて電子データに対する暗号処理が行われ、ステップＳ９で通信処理部１８から電子データの送信が行われて、処理を終了する。

【００３３】

ステップＳ６でグループ内のデータ送受信でない場合には、ステップＳ１１で

異なるグループに属する電子データ保管装置との間でのデータの送受信であるか否かが判定され、データ送受信でない場合にはそのまま処理を終了する。異なるグループに属する電子データ保管装置との間でのデータ送受信である場合には、ステップＳ１２で鍵管理部１２によって公開鍵保持部１６から公開鍵が選択され、ステップＳ８で公開鍵を用いて暗号処理が行われ、ステップＳ９でデータが送信されて、処理を終了する。

【００３４】

図４は、図３におけるグループ内データ送受信処理の詳細フローチャートである。同図において、ステップＳ１５で送信側の電子データ保管装置に対してグループ内通信指示が与えられると、ステップＳ１６でデータ保管部１７から送信すべきデータが選択され、ステップＳ１７で鍵管理部１２によって個別鍵保持部１４の保持する個別鍵が選択され、ステップＳ１７で鍵管理部１２によって個別鍵保持部１４の保持する個別鍵が選択され、ステップＳ１８で暗号処理部１３によって個別鍵を用いて電子データの復号とその内容の検証が行われる。この暗号処理部による処理については後述する。

【００３５】

電子データ検証の結果、電子データの改ざんが行われていないことが判明すれば、ステップＳ１９で鍵管理部１２によってグループ鍵保持部１５に保持されているグループ鍵が選択され、ステップＳ２０で暗号処理部１３によってグループ鍵を用いて電子データに対する暗号処理が行われ、ステップＳ２１で通信処理部１８によって受信側の電子データ保管装置に対するデータ送信が行われる。

【００３６】

受信側の電子データ保管装置においては、通信処理部１８によってステップＳ２４でデータが受信され、ステップＳ２５で鍵管理部１２によってグループ鍵保持部１５が保持するグループ鍵が選択され、ステップＳ２６で暗号処理部１３によってグループ鍵を用いて電子データの復号とその内容の検証が行われる。

【００３７】

検証の結果、電子データが改ざんされていないことが判明すると、ステップＳ２７で鍵管理部１２によって個別鍵保持部１４が保持する個別鍵が選択され、ス

テップＳ２８で暗号処理部１３によって個別鍵を用いて電子データに対する暗号処理が行われ、ステップＳ２９でデータ保管部１７にデータが保管されて、処理を終了する。

【００３８】

図５は異なるグループに属する電子データ保管装置との間での電子データ送受信の詳細処理フローチャートである。図４のグループ内の電子データ保管装置との間でのデータ送受信の処理フローチャートと異なる部分を中心に説明する。まず送信側の電子データ保管装置において、ステップＳ３１で異なるグループに属する電子データ保管装置との間での通信指示が受け取られ、図４におけると同様にステップＳ１６～Ｓ１８の処理が行われる。その後ステップＳ３２で鍵管理部１２によって公開鍵保持部１６に保持されている公開鍵が選択され、ステップＳ３３でその公開鍵を用いて暗号処理が行われ、その結果はステップＳ２１で受信側の電子データ保管装置に向けて送信される。

【００３９】

受信側の電子データ保管装置においては、ステップＳ２４でデータを受信した後、ステップＳ３６で鍵管理部１２によって公開鍵保持部１６に保持されている公開鍵と対となる秘密鍵が選択され、ステップＳ３７で暗号処理部１３によって公開鍵暗号アルゴリズムを用いてデータの復号、および内容の検証が行われる。電子データの改ざんが行われていないことが検証されると、図４におけると同様にステップＳ２７～Ｓ２９の処理が行われ、処理を終了する。ここで電子文書には送信側の秘密鍵による電子署名と受信側の公開鍵による暗号文を同時に送るようなＰＥＭ（プライバシ・エンハンスド・メール）のような一般的な方法を用いてもよいし、送信側と受信側の公開鍵によって、Ｄ－Ｈ法（ディフィー・ヘルマン法）によってセッション鍵を一時的に共有して通信を行ってもよい。

【００４０】

図４、および図５で説明したように、グループ内、または異なるグループに属する電子データ保管装置との間でデータの送受信を行う場合には、送信側において個別鍵によって暗号処理されて保管されているデータを、グループ内ではグループ鍵、異なるグループの場合には公開鍵によって暗号処理をし直して送信し、

受信側ではグループ内ではグループ鍵、異なるグループとの間では公開鍵を用いてデータの検証を行った後、個別鍵で暗号処理し直して保管することによって、例えばグループ鍵が暴露されると危険に犯されたとしても、各保管装置内部に保管されている電子データの安全性を保つことが可能となる。

【００４１】

続いて各電子データ保管装置に保持されている鍵の生成、および管理について、図６～図１０を用いて、その処理フローチャートを説明する。図６は各電子データ保管装置の個別鍵があらかじめ割り当てられている場合のデータ保管処理のフローチャートである。あらかじめ電子データ保管装置に割り当てられている鍵とは、例えば電子データ保管装置の工場出荷時に各装置に割り当てられる鍵のことであり、メーカによって管理されるため、メーカ鍵を呼ぶことにする。

【００４２】

図６において、工場出荷時にステップＳ４０でメーカによって鍵管理機能付電子データ保管装置が作成されて、ステップＳ４１でメーカによってその電子データ保管装置に対するメーカ鍵が作成され、ステップＳ４２でそのメーカ鍵が個別鍵保持部１４に設定された後、電子データ保管装置が出荷される。このメーカ鍵は電子データ保管装置の識別情報、例えばＩＤなどと組み合わせて、メーカによって管理される。

【００４３】

電子データ保管装置の利用時には、ステップＳ４４で電子データが受信され、ステップＳ４５で鍵管理部１２によって個別鍵保持部１４に保持されているメーカ鍵が選択され、ステップＳ４６で暗号処理部１３によってメーカ鍵を用いて電子データの暗号処理が行われ、ステップＳ４７でデータ保管部１７にデータが保管されて、処理を終了する。

【００４４】

このように電子データ保管装置の個別鍵としてメーカによって管理されるメーカ鍵を用いることによって、利用者は鍵の管理をする必要がなくなり、また利用者側での鍵の暴露を最小限にすることができる。また利用者側の電子データ保管装置の暗号処理部１３が壊れても、メーカによって管理されているメーカ鍵を用

いて電子データ保管装置内のデータを再構築することも可能となる。

【００４５】

図７はグループの中の主となる電子データ保管装置、例えばグループマスタによるグループ内の電子データ保管装置の個別鍵の管理処理のフローチャートである。同図において処理が開始されると、まずステップＳ５０で複数の電子データ保管装置によって構成されるグループの中で主となる保管装置、例えばグループマスタが決定され、Ｓ５１でそのグループマスタの鍵を用いてグループに属する個々の保管装置の個別鍵が作成され、ステップＳ５２でグループマスタが作成した個々の保管装置の個別鍵が配布され、ステップＳ５３で個々の電子データ保管装置は個別鍵保持部１４に配布された鍵を設定して、処理を終了する。グループマスタによる各個別鍵の生成、およびその配布の方法についいは後述する。

【００４６】

図８は２つの鍵を関連付けて個別鍵を生成する処理のフローチャートである。２つの鍵とは、例えば電子データ保管装置にあらかじめ割り当てられている鍵と、新たに指定される鍵であり、あらかじめ割り当てられている鍵は、例えば前述のメーカ鍵であり、新たに指定される鍵とは電子データ保管装置を利用する管理者によって設定される鍵であり、管理者鍵と呼ばれるものである。管理者は利用者（ユーザ）と異なって、個別鍵、グループ鍵の設定をすることができるが、利用者は、電子データの保管、参照、および転送などしか行うことができない。

【００４７】

図８において、ステップＳ５５で管理者によって新たに個別鍵の生成の指示が与えられると、ステップＳ５６で管理者によって管理者鍵が指定され、ステップＳ５７で暗号処理部１３によって前述のメーカ鍵と管理者鍵とが関連づけられて個別鍵が生成され、ステップＳ５８で鍵管理部１２によって個別鍵保持部１４に生成された個別鍵が設定されて、処理を終了する。メーカ鍵と管理者鍵との関連づけによる個別鍵の生成については後述する。

【００４８】

このように電子データ保管装置の個別鍵の生成にあたってメーカ鍵と管理者鍵とを関連づけることにより、管理者が組織の変更やグループの構築など、環境や

運用形態に合わせて、電子データ保管装置を管理することができる。また暗号処理部が壊れた場合などに、前述と同様にメーカがデータの再構築や検証を行うことも可能である。

【００４９】

図９はグループマスタによるグループ鍵管理処理のフローチャートである。グループ鍵は、前述のように１つのグループ内での電子データの送受信に対して用いられるものであり、図９のフローチャートは図７のグループマスタによる個別鍵の管理処理のフローチャートと同様である。

【００５０】

すなわちステップＳ６０でグループマスタが決定された後、ステップＳ６１でグループマスタによってグループ鍵が生成され、ステップＳ６２でそのグループ鍵がグループ内の電子データ保管装置に配布され、ステップＳ６３で各電子データ保管装置はグループ鍵保持部１５に配布されたグループ鍵を設定して、処理を終了する。

【００５１】

図１０は、図８と同様に、２つの鍵を関連づけてグループ鍵を生成する処理のフローチャートである。図８におけると同様に、２つの鍵とはメーカ鍵と管理者鍵のことである。

【００５２】

図１０の最初の２つのステップは図８におけると同様である。その後、ステップＳ６６で暗号処理部１３によってメーカ鍵と管理者鍵とが関連づけられてグループ鍵が生成され、ステップＳ６７で鍵管理部１２によってグループ鍵保持部１５にグループ鍵が設定され、ステップＳ６８でグループに属する電子データ保管装置にグループ鍵が配布されて、処理を終了する。なおこのフローチャートの処理は、例えば前述のグループマスタによって行われるものである。

【００５３】

図１１は本発明の第２の実施の形態における鍵管理機能付電子データ保管装置の構成ブロック図である。第１の実施の形態における図２と比較すると、全ての電子データ保管装置に共通の鍵であるマスタ鍵を保持するマスタ鍵保持部２０が

追加されている点だけが異なっている。

【００５４】

図１２は第２の実施の形態におけるマスタ鍵を用いた個別鍵生成処理のフローチャートである。同図において、ステップＳ７０で個別鍵の生成指示を受け取ると、ステップＳ７１で制御部１１によって自装置の識別情報、例えば電子データ保管装置のＩＤが取得され、ステップＳ７２で鍵管理部１２によってマスタ鍵保持部２０に保持されているマスタ鍵が取得され、ステップＳ７３で暗号処理部１３によって電子データ保管装置識別情報がマスタ鍵を用いて暗号化されて、個別鍵が生成される。この暗号化処理については後述する。そして、ステップＳ７４で鍵管理部１２によって、個別鍵保持部１４に生成された個別鍵が設定されて処理を終了する。

【００５５】

このように全ての電子データ保管装置に共通のマスタ鍵を用いて個々の電子データ保管装置が個別鍵を生成することによって、個々の保管装置による自動的な個別鍵生成が可能となる。また電子データ保管装置のメーカは、暗号処理部が壊れた時などに電子データ保管装置の識別情報を参照することにより、保管されているデータ検証や再構築を行うことが可能となる。

【００５６】

図１３は第２の実施の形態におけるグループ鍵生成とその配布処理のフローチャートである。なおこの処理ではマスタ鍵は使用されないため、第１の実施の形態においても同様の処理を実行することが可能である。

【００５７】

図１３のステップＳ７５でグループ鍵作成指示がグループマスタに与えられると、ステップＳ７６でグループマスタの制御部１１によってグループ識別情報が取得される。このグループ識別情報は、そのグループマスタが管理するグループを識別するためのＩＤである。そしてＳ７７で鍵管理部１２によって個別鍵保持部１４に保持されている個別鍵が選択され、ステップＳ７８で暗号処理部１３によってグループ識別情報が個別鍵で暗号化されてグループ鍵が生成され、ステップＳ７９で生成されたグループ鍵が通信処理部１８からグループ内の電子データ

保管装置に配布される。

【００５８】

グループマスタによって管理される、グループに属する保管装置側では、ステップＳ８０ａにおいて通信処理部１８によってグループ鍵が受信され、ステップＳ８０ｂで鍵管理部１２によってグループ鍵保持部１５にグループ鍵が設定されて処理を終了する。

【００５９】

図１４はグループ管理電子データ保管装置によるグループマスタの個別鍵生成処理のフローチャートである。グループ管理電子データ保管装置とは、複数のグループ内でそれぞれ主となる電子データ保管装置、すなわち複数のグループマスタを管理するものであり、グループ管理電子データ保管装置はグループマスタを管理するものであり、グループ管理電子データ保管装置はグループマスタ個々に対する個別鍵を生成して、グループマスタに配布する。

【００６０】

ステップＳ８２でグループマスタの個別鍵の生成指示が受け取られ、ステップＳ８３で複数の各グループに対するグループ識別情報が指定され、ステップＳ８４で鍵管理部１２によって個別鍵保持部１４に保持されている個別鍵が選択され、ステップＳ８５で暗号処理部１３によって個別鍵を用いて各グループ識別情報が暗号化され、各グループマスタに対する個別鍵が生成され、ステップＳ８６で各グループマスタに個別鍵が配布されて、処理を終了する。

【００６１】

次にグループの階層化について説明する。例えば図３では、それぞれ複数の電子データ保管装置によって構成される複数のグループはお互いに対等なものとして、本発明の第１の実施形態、および第２の実施形態を説明したが、グループの間に上位のグループと下位のグループとの階層関係が存在する場合を図１５に示す。

【００６２】

図１５において、上位グループは管理グループとしての下位のグループを管理しており、上位グループに属する電子データ保管装置（ＳＡ）は、例えば自グル

ープに対する上位グループ鍵と、管理グループに対する下位グループ鍵を保持しているものとする。これに対して下位グループに属する電子データ保管装置は自グループに対する下位グループだけを保持するものとする。そして例えば上位グループの中で、下位グループの電子データ保管装置を管理する下位グループマスタＳＡが、下位グループ鍵を作成して、下位グループのＳＡに配布するものとする。ここでＳＡはセキュア・アーカイバの略号であり、電子データ保管装置である。

【００６３】

図１６は階層関係にある２つのグループにおける通信方法の説明図である。上位グループの中でのＳＡ同志の通信は上位グループ鍵を用いて行われ、下位グループの中でのＳＡ同志の通信は下位グループ鍵を用いて行われる。上位グループのＳＡ、例えばＳＡ１と下位グループのＳＡ、例えばＳＡ２との間の通信は上位グループ中のＳＡの１つであり、下位グループのＳＡを管理する下位グループマスタＳＡを介して行われるものとする。下位グループマスタＳＡと下位グループに属するＳＡ、例えばＳＡ２との間の通信は下位グループ鍵を用いて行われるものとする。

【００６４】

この下位グループマスタＳＡがある組織の管理部に属しているものとすれば、管理部のＳＡが各部門等のＳＡの個別鍵やグループ鍵を生成、配布、管理することによりグループの階層化が実現され、また各ＳＡに保管されているデータを管理部から検証することが可能となる。

【００６５】

図１７は、図１６において、例えば上位グループのＳＡ１から下位グループのＳＡ２への通信処理のフローチャートである。同図において、ステップＳ９１で上位グループのＳＡ１に対して下位グループのＳＡ２に対するデータの転送が指示されると、ステップＳ９２で、例えば図２の鍵管理部１２によって個別鍵保持部１４の保持する個別鍵が選択され、、ステップＳ９３で暗号処理部１３によって個別鍵を用いてデータの復号と検証が行われ、ステップＳ９４で鍵管理部１２によってグループ鍵保持部１５に保持されている上位グループ鍵が選択され、ス

テップＳ９５で暗号処理部１３によって上位グループ鍵を用いて電子データに対する暗号処理が行われ、ステップＳ９６で通信処理部１８から暗号処理された電子データが下位グループマスタＳＡに転送される。

【００６６】

下位グループマスタＳＡ側では、ステップＳ９７で通信処理部１８によって暗号処理されたデータが受信され、ステップＳ９８で鍵管理部１２によってグループ鍵保持部１５に保持されている上位グループ鍵が選択され、ステップＳ９９で暗号処理部１３によって上位グループ鍵を用いて電子データの復号と検証が行われ、ステップＳ１００で鍵管理部１２によってグループ鍵保持部１５に保持されている下位グループ鍵が選択され、ステップＳ１０１で暗号処理部１３によって下位グループ鍵を用いてデータに対する暗号処理が行われ、ステップＳ１０２で通信処理部１８によって暗号処理されたデータが下位グループのＳＡ２に転送される。

【００６７】

下位グループのＳＡ２においては、ステップＳ１０３で通信処理部１８によって暗号処理鍵されたデータが受信され、ステップＳ１０４で鍵管理部１２によってグループ鍵保持部１５に保持されている下位グループ鍵が選択され、ステップＳ１０５で暗号処理部１３によって下位グループ鍵を用いてデータの復号と検証が行われ、ステップＳ１０６で鍵管理部１２によって個別鍵保持部１４に保持されている個別鍵が選択され、ステップＳ１０７で暗号処理部１３によって個別鍵を用いてデータに対する暗号処理が行われ、ステップＳ１０８で制御部１１によってデータ保管部１７にデータが保管されて、処理を終了する。

【００６８】

図１８は、図１７とは逆に、下位グループのＳＡ２から上位グループのＳＡ１へのデータ送信処理のフローチャートである。同図の処理は図１７とほぼ逆になるだけであり、データ送信側のＳＡ２では個別鍵と下位グループ鍵を用いて処理が行われ、下位グループマスタＳＡでは下位グループ鍵を用いてデータの復号と検証が行われた後、上位グループ鍵を用いてデータに対する暗号処理が行われ、受信側のＳＡ１では上位グループ鍵と個別鍵とを用いて処理が行われることにな

る。

【００６９】

なお図１７の説明に図２の第１の実施の形態における電子データ保管装置の構成を用いたが、図１７および図１８の処理は、図１１で説明した第２の実施の形態における電子データ保管装置においても全く同様に行われる。

【００７０】

次に個別鍵を用いた電子データ（電子文書）の保管、グループ内におけるグループ鍵の利用方法、電子データに対する改ざん検出情報（ＭＡＣ、メッセージオーセンティフィケーションコード）の作成、鍵の生成などについて説明する。

【００７１】

図１９は個別鍵を利用した電子文書保管の説明図である。同図において、①で電子文書の保管指示が電子データ保管装置に与えられると、保管装置において②で個別鍵と電子文書を用いてＭＡＣが構成され、③でＭＡＣと電子文書が保管される。

【００７２】

図２０は同一グループ内の２つの電子データ保管装置ＡとＢの間での通信方法の説明図である。同図において、送信側のデータ保管装置Ａ側では、①でＭＡＣの再計算が行われて、電子文書の検証が行われた後に、②でグループ鍵と電子文書に対応してＭＡＣが計算され、③でそのＭＡＣと電子文書が保管装置Ｂ側に送信される。

【００７３】

電子データ保管装置Ｂ側では、④４でＭＡＣと電子文書を受信し、⑤でＭＡＣの内容をグループ鍵を用いて検証し、検証結果が正しければ、⑥で個別鍵と電子文書に対応してＭＡＣが計算され、⑦で計算されたＭＡＣと電子文書が保管される。

【００７４】

図２１は、図１９，図２０で説明した電子データに対する改ざん検出情報ＭＡＣの計算方法の説明図である。ＭＡＣの計算においては、アメリカの規格協会によって採用された暗号化法としてのＤＥＳ（データエンクリプションスタンダー

ド）が用いられる。この暗号化法では、暗号化／復号化を１つのＬＳＩで処理することができる。

【００７５】

図２１において、まず元データが６４ビットずつのブロックＭ１，Ｍ２，・・・Ｍｎに分割される。そして、まず最初のブロックＭ１、６４ビットに対するＤＥＳ処理が、鍵、例えば個別鍵を用いて行われ、その結果の６４ビットのデータと次のブロックＭ２、６４ビットとの排他的論理和が求められる。

【００７６】

さらにその結果に対して、例えば個別鍵を用いて再びＤＥＳ処理が行われ、６４ビットの結果が得られる。以後同様の処理が行われ、最終的に得られる６４ビットのうちで、上位３２ビットが改ざん検出情報ＭＡＣとして求められる。なお改ざん検出情報ＭＡＣの計算は、ここで示した方法に限定されるものではなく、他のアルゴリズムを用いてもよい。

【００７７】

図２２は一般的な鍵の生成法の説明図である。同図において、例えば前述のグループマスタがグループに属する電子データ保管装置の個別鍵を生成して配布する場合には、個々の保管装置を識別する情報、例えばＩＤとシード鍵としてのグループマスタの個別鍵を用いてＤＥＳ処理を行い、個々の保管装置に対応する個別鍵を、ニュー鍵として生成して配布することができる。前述のように例えばメーカ鍵と管理者鍵の２つの鍵を関連づけて新たな鍵を生成する場合も全く同様である。

【００７８】

この個別鍵の配布の方法としては、鍵配布サーバを用いたり、公開鍵をベースとした認証基盤に基づくＧＫＭＦ（グループキーマネージメントフレームワーク）を用いてオンラインで配布してもよく、フロッピーやＩＣカードなどの媒体を用いてオフラインで配布することもできる。

【００７９】

ここで、ＧＫＭＦは公開鍵認証基盤の証明書を各グループメンバが持つことによって鍵の設定や更新等の管理を行うものである、また公開鍵をベースとした認

証基盤とは信頼のおける第３者としての認証局を信頼点とすることによって、各個人が公開鍵に対して第３者のお墨付き（電子署名）を受けることによって、２者の間の認証を行う枠組みである。

【００８０】

図２３はグループ鍵の生成とその配布の説明図である。同図において、２つのグループ１，２が存在し、各グループはグループマスタの配下に、例えば３つのＳＡを備えているものとする。図２３では、例えばグループマスタは自装置の個別鍵、Ｉ鍵と自装置のＩＤとを用いて、まずグループマスタ鍵（Ｇｍ 鍵）を生成し、その後このＧｍ 鍵とグループに対するＩＤを用いてグループ鍵、Ｇ鍵を生成し、このグループ鍵を配下のＳＡに配布する。

【００８１】

このグループ鍵は各ＳＡ内のグループ鍵保持部に保持されるが、グループ鍵はグループを識別するＩＤと鍵のペアで管理されており、例えば１つのＳＡが複数のグループに属したり、図１６で説明した下位グループマスタＳＡのように上位グループ鍵と下位グループ鍵とを保持する必要があるために、グループ鍵とグループを識別するＩＤのペアーが一般に複数保持されることになる。またグループ鍵とＩＤのペアの他に、グループに含まれるデータ保管装置のＩＰアドレスや、名前などの属性を同時に管理してもよい。

【００８２】

また図２３において、グループ１とグループ２の間の通信はセッション鍵（Ｓ鍵）を用いて行われている。このセッション鍵は、公開鍵証明書に基づいて、例えばグループマスタ相互間で共通される秘密鍵である。公開鍵は、一般に異なる複数のグループとの間の通信を行うためにグループ鍵と同様に複数、例えばグループマスタによって管理され、国際電気通信連合のＩＴＵ－ＴＸ５０９に示される公開鍵証明書の形式を用いて、信頼のおける第３者が認証を確認できる形態で、保存されてもよい。

【００８３】

図２４は、それぞれ複数のＳＡによって構成されるグループが複数存在する場合の、グループ管理ＳＡによる全体管理方法の説明図である。同図においてグル

ープＡ，Ｂ，Ｃの３つのグループが構成されており、それぞれのグループ内で主となる電子データ保管装置、すなわちグループマスタＳＡが存在する。

【００８４】

グループ管理ＳＡは（グループ管理電子データ保管装置）は各グループのグループマスタＳＡを管理するものであり、例えば図１４で説明したようにグループマスタＳＡの個別鍵を生成して各グループマスタＳＡに配布するような処理を実行する。このように複数のグループを管理するグループ管理ＳＡが存在することによって、インターンネットのようなグローバルなネットワーク環境でも、不特定多数のグループのいずれのグループをも相手とする通信が可能となる。

【００８５】

最後に、本発明の鍵管理機能付電子データ保管装置どを実現するためのプログラムのコンピュータへのローディングについて、図２５を用いて説明する。同図において、セキュアな筐体内のコンピュータ２５は本体２６とメモリ２７とから構成されており、本体２６に対してはセキュアな可搬型記憶媒体２９からプログラムなどをロードすることも、またプログラム提供者側からネットワーク２８を介してプログラムなどをロードすることも可能である。

【００８６】

本発明の特許請求の範囲における電子データ保管装置内の各種の処理や、電子データ保管装置相互間でのデータ送受信などのためにプログラムや、各フローチャートに示されているプログラムなどは、例えばセキュアなメモリ２７に格納され、そのプログラムは本体２６によって実行される。ここでセキュアなメモリ２７としては、ハードディスクなどが用いられる。

【００８７】

また例えば電子ディスク保管装置相互間でのデータ送受信のためのプログラムなどは、セキュアな可搬型記憶媒体２９に記憶され、セキュアな筐体内のコンピュータ２５にそのプログラムをロードすることによって、通信を行うことも可能である。このセキュアな可搬型記憶媒体２９としては、セキュアなメモリカード、フロッピーディスク、ＣＤ／ＲＯＭ、光ディスク、光磁気ディスクなどを用いることができる。さらにデータ通信のためのプログラムなどは、プログラム提供

者側からネットワーク２８を介してセキュアな筐体内のコンピュータ２５側に送られ、そのプログラムがロードされることによってデータの通信を実現することも可能である。

【００８８】

以上において本発明の実施の形態を詳細に説明したが、本発明の実施の形態は以上の記述に限定されることなく、特許請求の範囲に記載された範囲内で様々な実施形態を取ることができることは当然である。

【００８９】

【発明の効果】

以上詳細に説明したように、電子データ保管装置が鍵管理機能を備えることによって、利用環境に適した電子データの保管および送受信が可能となり、電子化された重要文書の安全性確保に寄与するとことが大きい。

【図面の簡単な説明】

【図１】

本発明の原理構成ブロック図である。

【図２】

本発明の第１の実施の形態における電子データ保管装置の構成を示すブロック図である。

【図３】

第１の実施の形態における電子データ保管装置の全体処理フローチャートである。

【図４】

同一グループに属する電子データ保管装置との間でのデータ送受信処理のフローチャートである。

【図５】

異なるグループに属する電子データ保管装置との間でのデータ送受信処理のフローチャートである。

【図６】

個別鍵があらかじめ割り当てられている場合の電子データ保管処理のフローチ

ャートである。

【図７】

グループマスタによる電子データ保管装置個別鍵の管理処理フローチャートである。

【図８】

２つの鍵を関連付けて個別鍵を生成する処理のフローチャートである。

【図９】

グループマスタによるグループ鍵管理処理のフローチャートである。

【図１０】

２つの鍵を関連づけてグループ鍵を生成する処理のフローチャートである。

【図１１】

第２の実施の形態における電子データ保管装置の構成を示すブロック図である。

【図１２】

第２の実施の形態におけるマスタ鍵を用いた個別鍵生成処理のフローチャートである。

【図１３】

第２の実施の形態におけるグループ鍵生成処理のフローチャートである。

【図１４】

グループ管理保管装置によるグループマスタの個別鍵生成処理のフローチャートである。

【図１５】

グループの階層化を説明する図である。

【図１６】

上位グループと下位グループの電子データ保管装置相互間での通信を説明する図である。

【図１７】

上位グループの保管装置から下位グループの保管装置へのデータ送信処理のフローチャートである。

【図１８】

下位グループの保管装置かた上位グループの保管装置へのデータ送信処理のフローチャートである。

【図１９】

個別鍵を用いた電子文書保管の説明図である。

【図２０】

同一グループに属する２つの保管装置の間でのデータ送受信を説明する図である。

【図２１】

改ざん検出情報ＭＡＣの計算方法を説明する図である。

【図２２】

鍵の生成方法の説明図である。

【図２３】

グループ鍵の生成とその配布を説明する図である。

【図２４】

それぞれ複数のＳＡによって構成されるグループが複数存在する場合の、グループ管理ＳＡによる全体管理方式の説明図である。

【図２５】

本発明の電子データ保管装置を実現するためのプログラムのコンピュータへのローディングを説明する図である。

【符号の説明】

１，１０，１９　　鍵管理機能付電子データ保管装置

２　　鍵管理手段

３　　暗号処理手段

１１　制御部

１２　鍵管理部

１３　暗号処理部

１４　個別鍵保持部

１５　グループ鍵保持部

１６　公開鍵保持部

１７　データ保管部

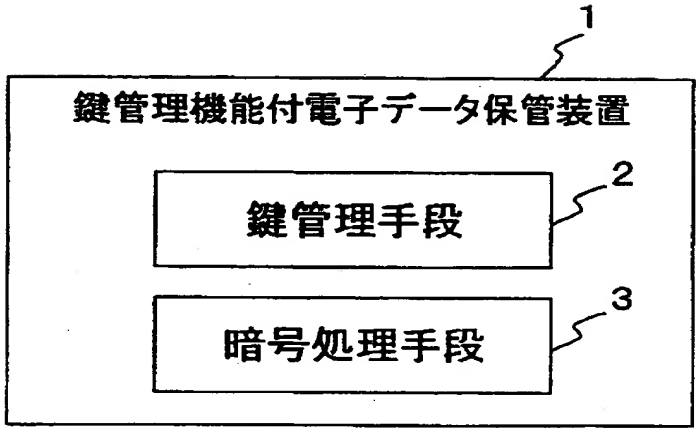
１８　通信処理部

２０　マスタ鍵保持部

【書類名】　　図面

【図１】

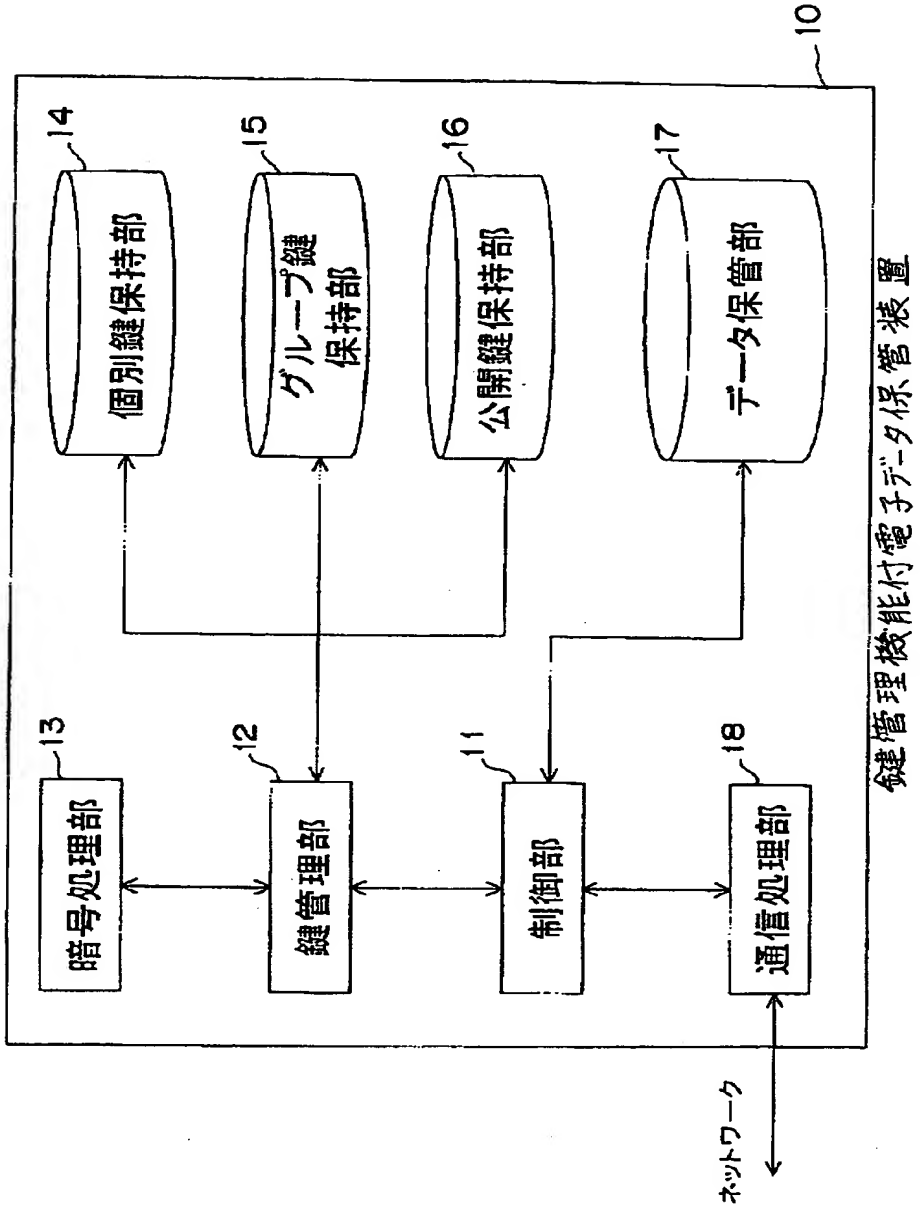
本発明の原理構成ブロック図



出証特平１１－３０１４８８１

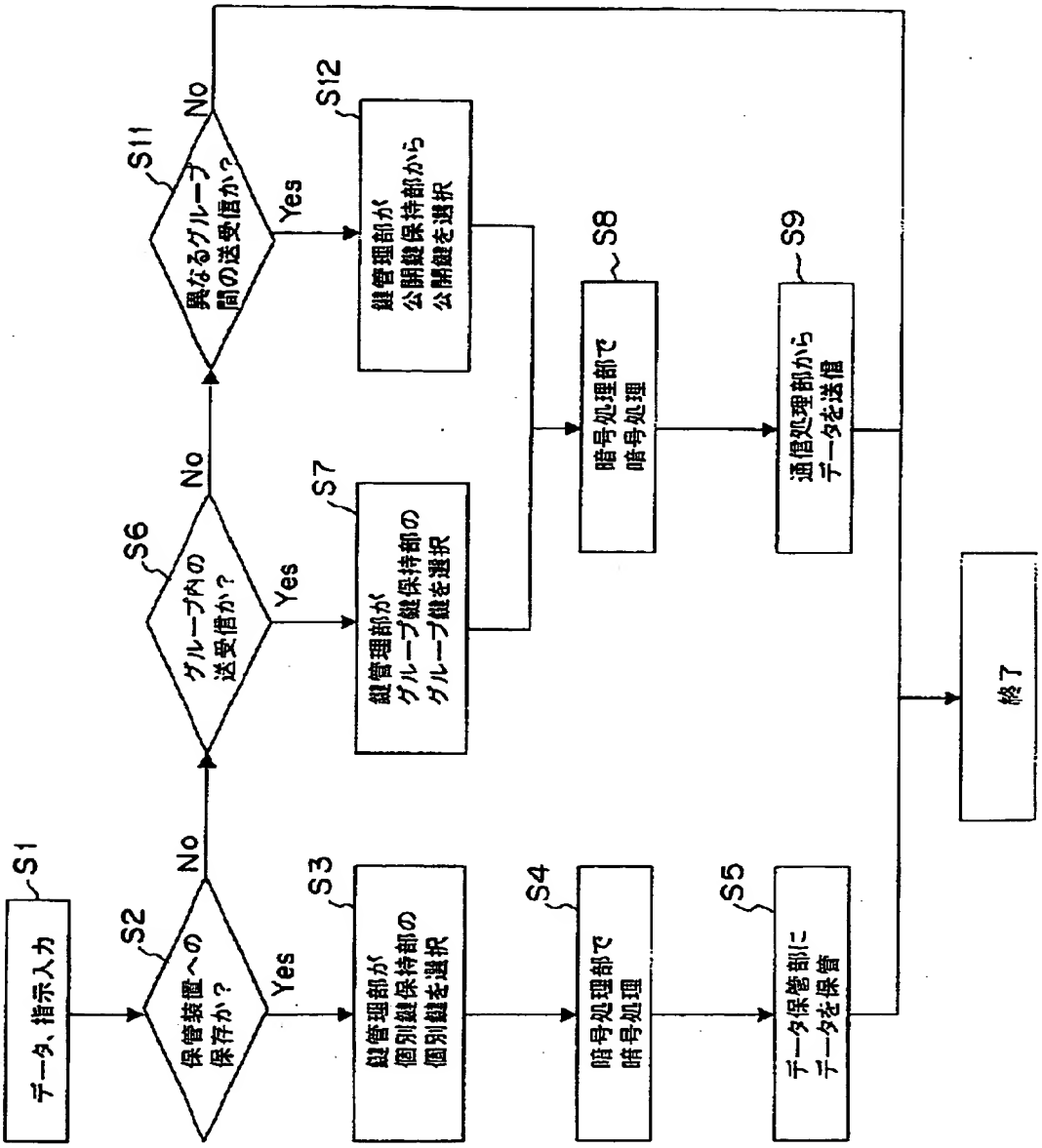
【図２】

本発明の第１の実施形態における
電子データ保管装置の構成を示すブロック図



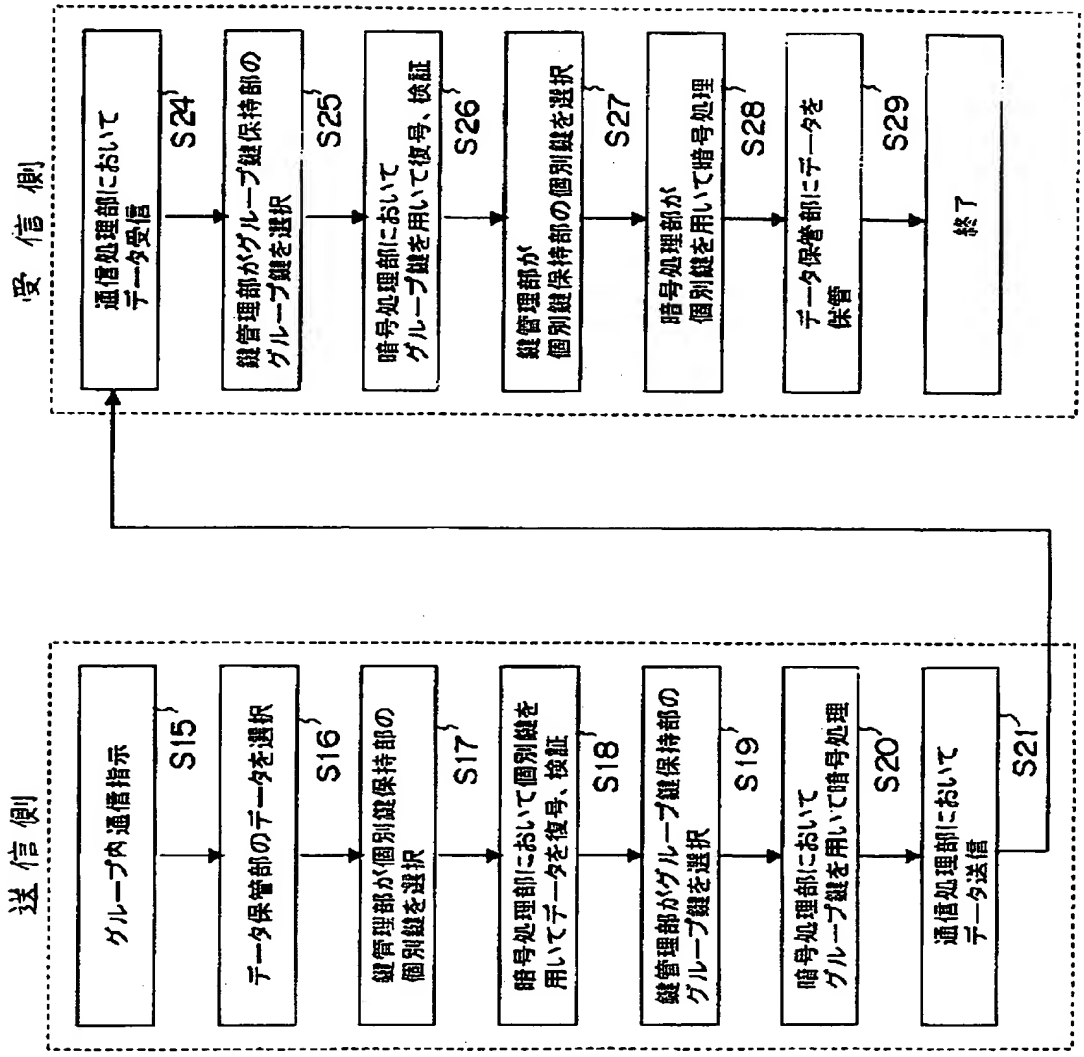
【図３】

第1の実施形態における電子データ保管装置の
全体処理フローチャート



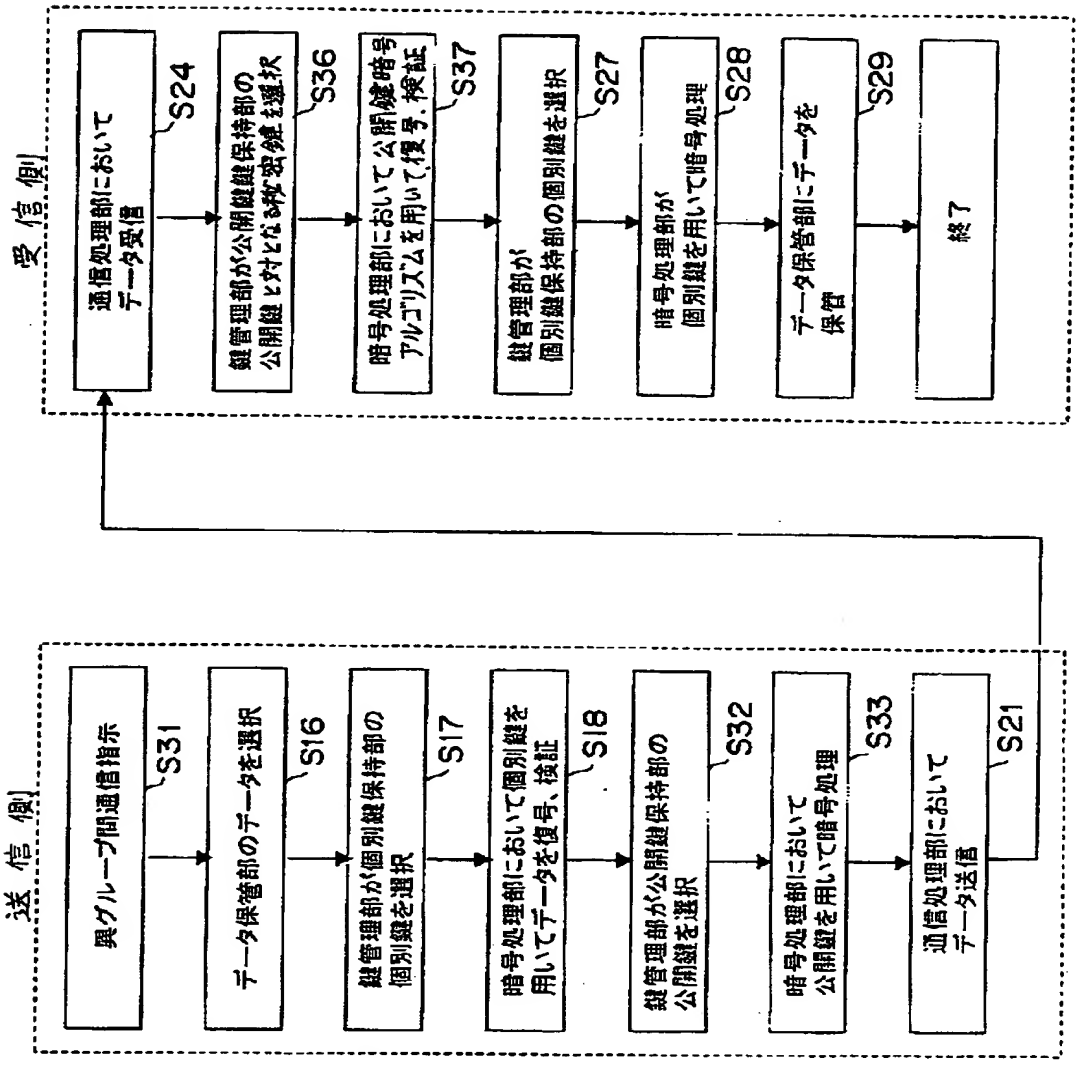
【図４】

同一グループに属する電子データ保管装置との間での
データ送受信処理のフローチャート



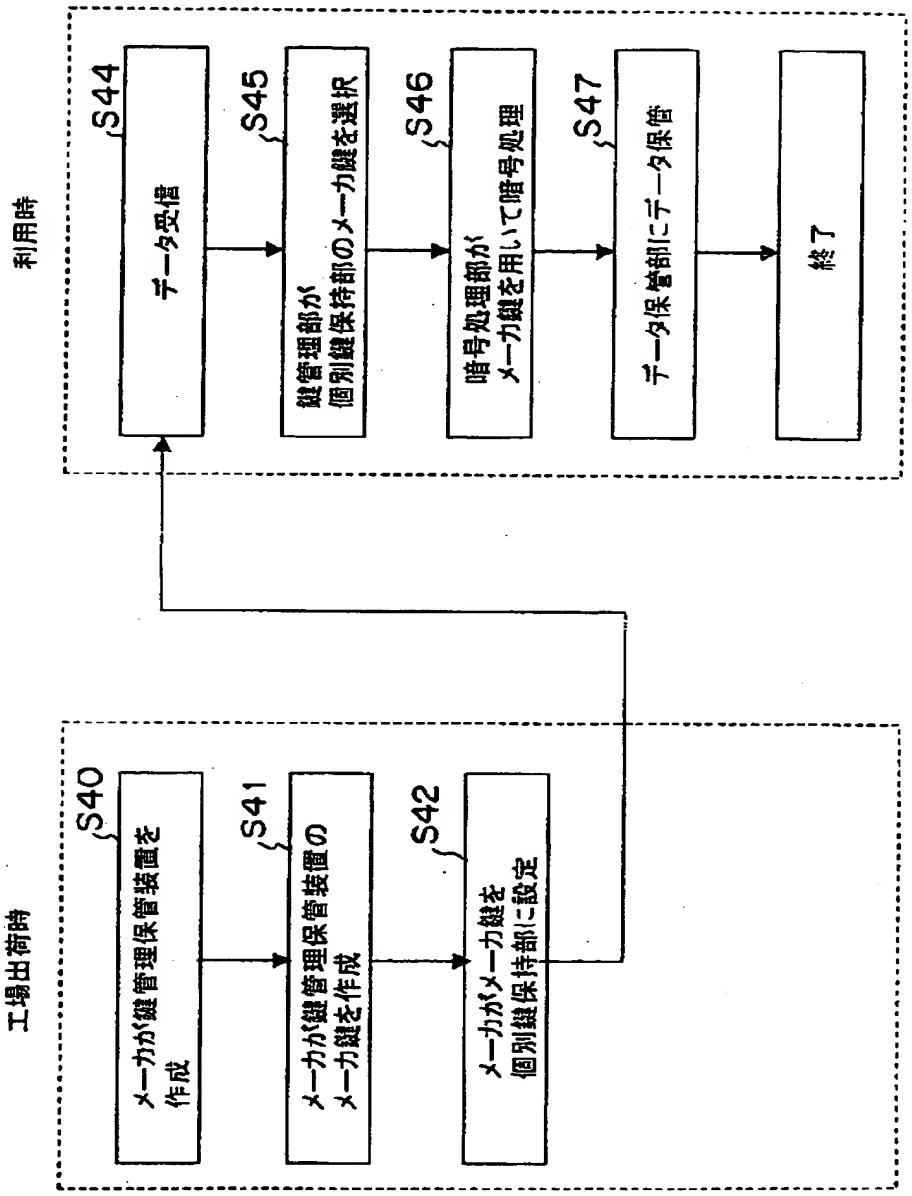
【図５】

異なるグループに属する電子データ保管装置との間でのデータ送受信処理のフローチャート



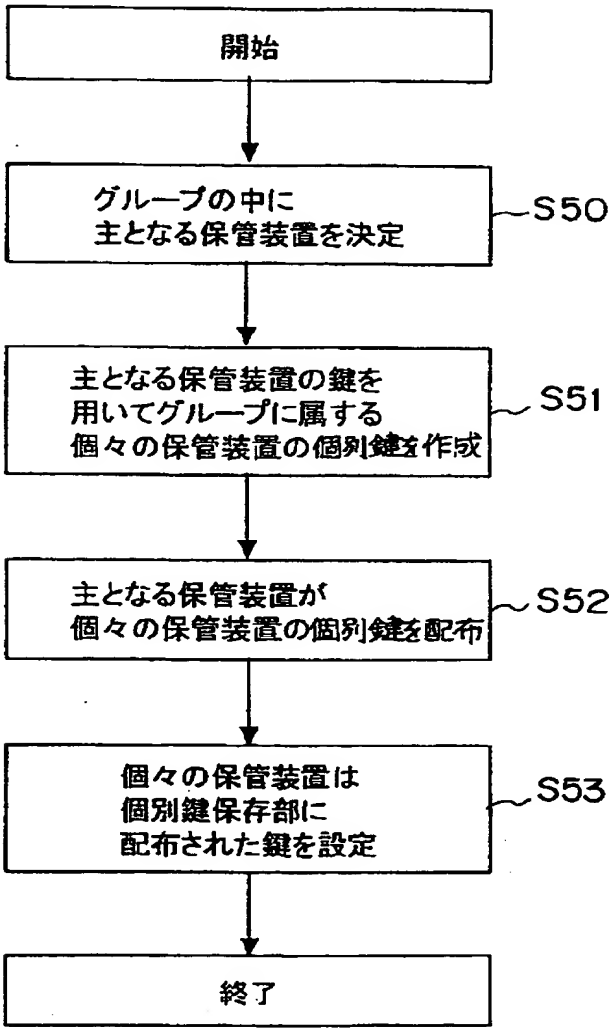
【図６】

個別キーがあらかじめ割当てられている場合の
電子データ保管処理のフローチャート



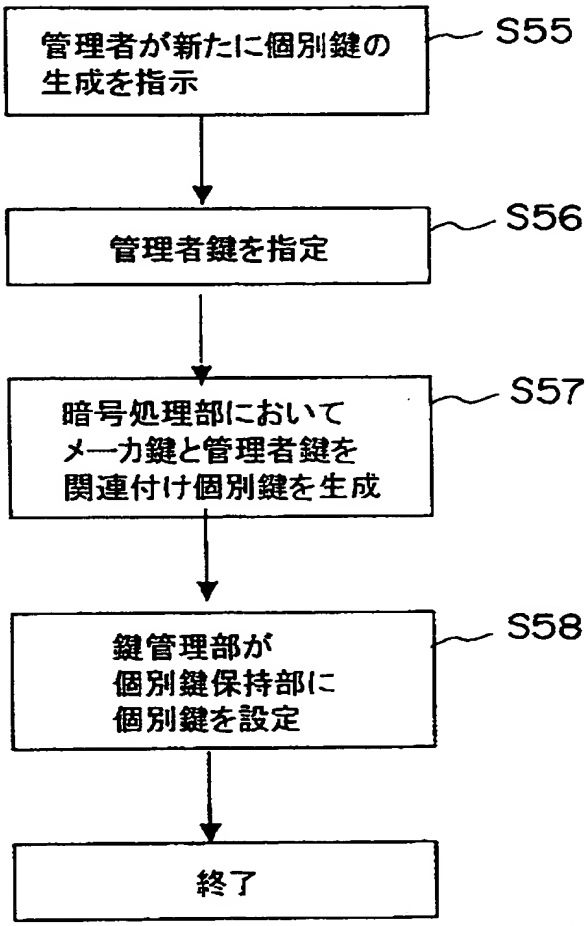
【図７】

グループマスタによる電子データ
保管装置個別鍵の管理処理フローチャート



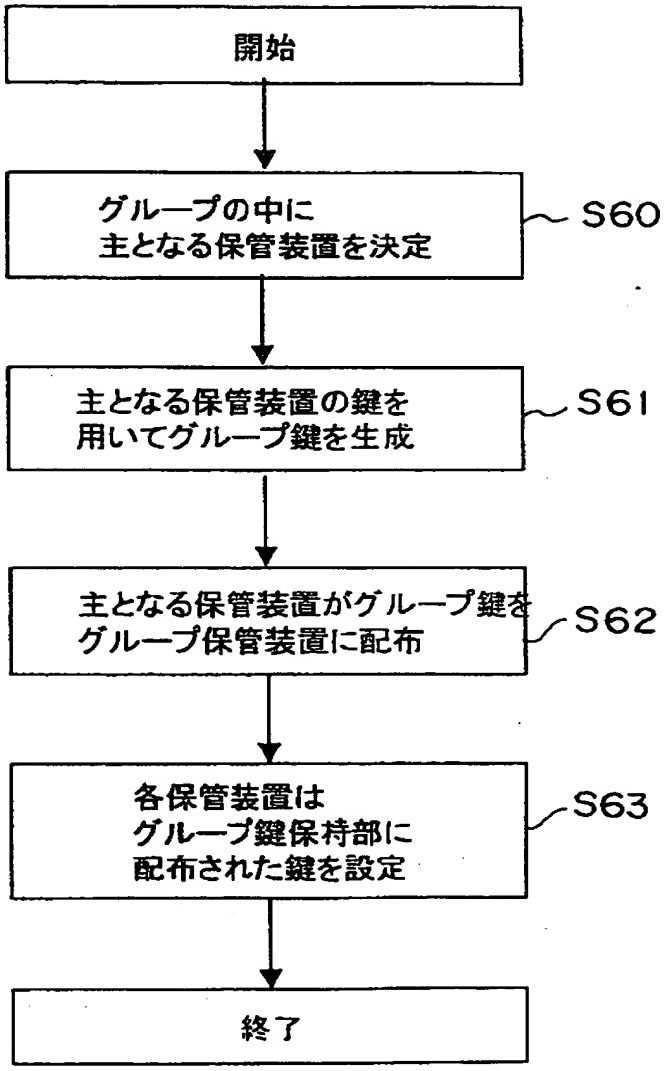
【図８】

２つの鍵を関連ずけて個別鍵を
生成する処理のフローチャート



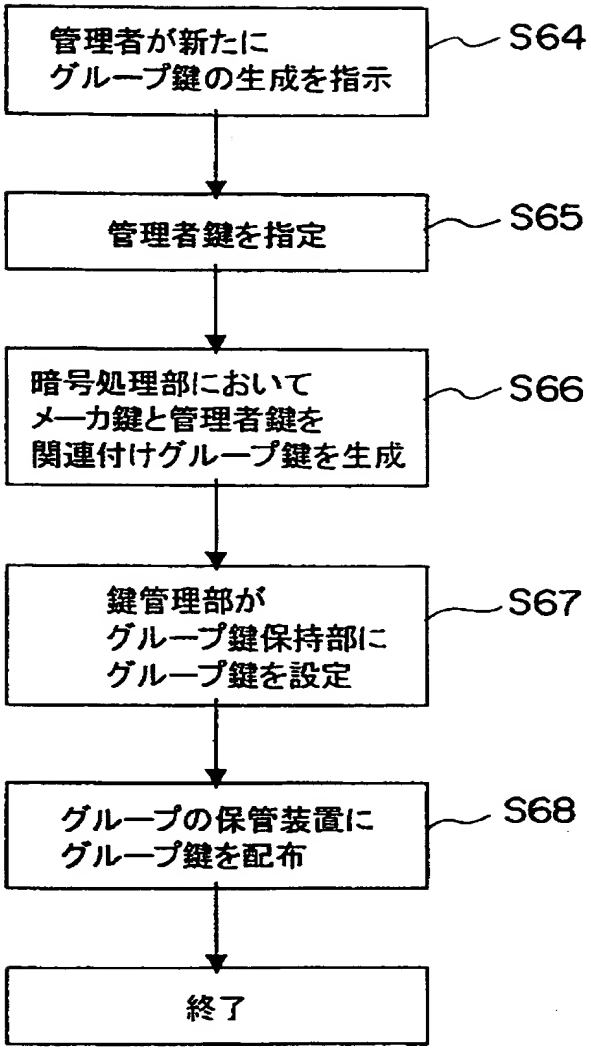
【図９】

グループマスタによるグループ鍵
管理処理のフローチャート



【図１０】

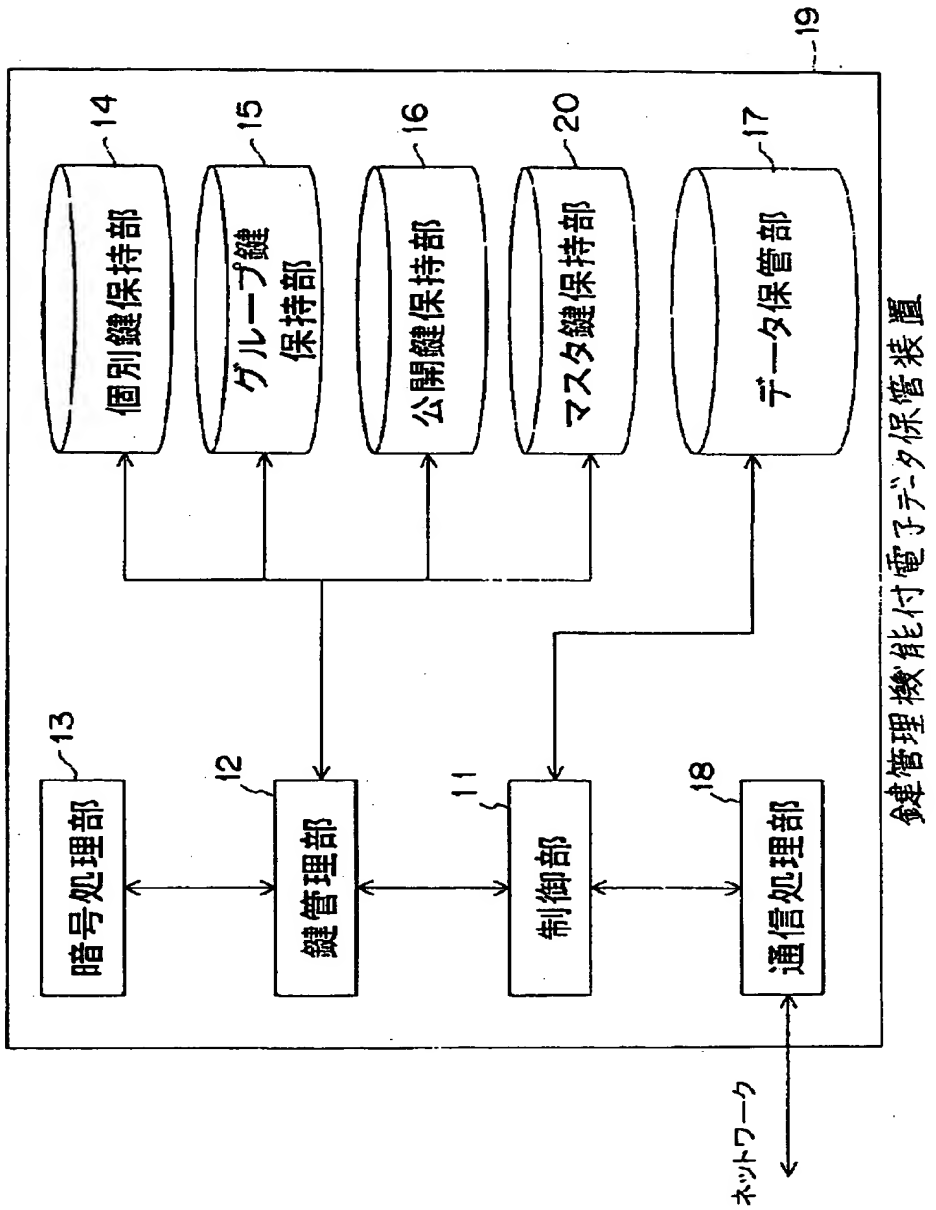
２つの鍵を関連づけてグループ鍵を生成する処理のフローチャート



出証特平１１－３０１４８８１

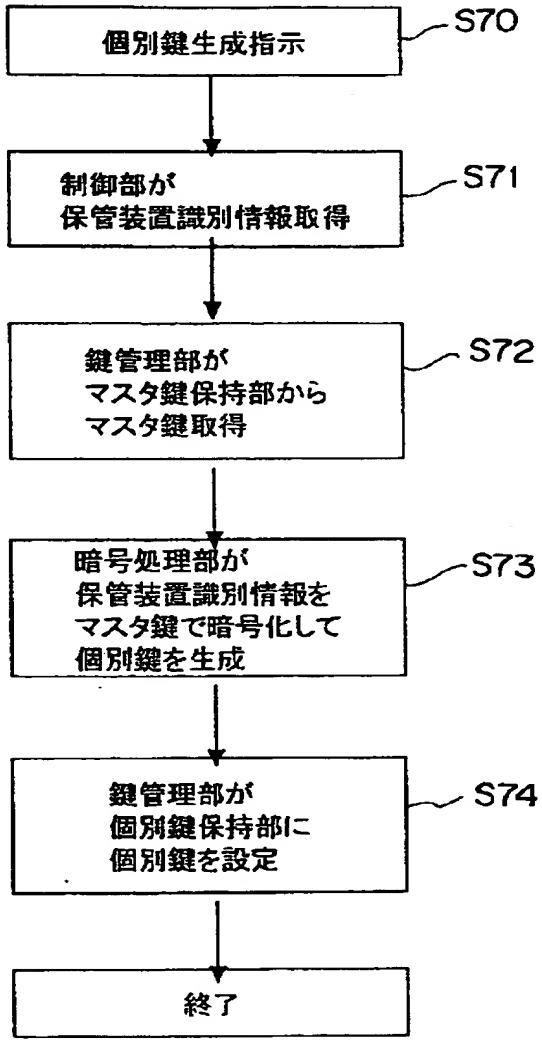
【図１１】

第2の実施形態における
電子データ保管装置の構成を示すブロック図



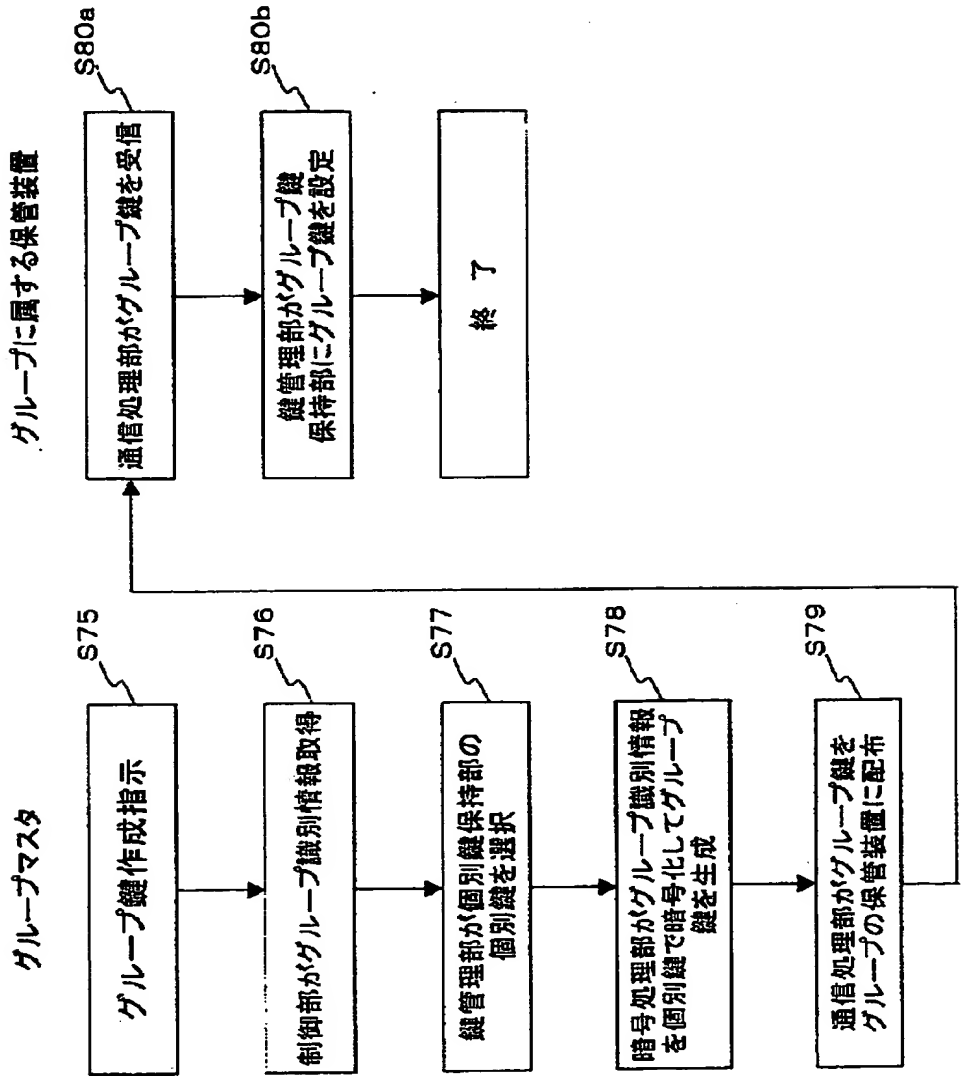
【図１２】

第２の実施形態における
マスタ鍵を用いた個別鍵生成処理のフローチャート



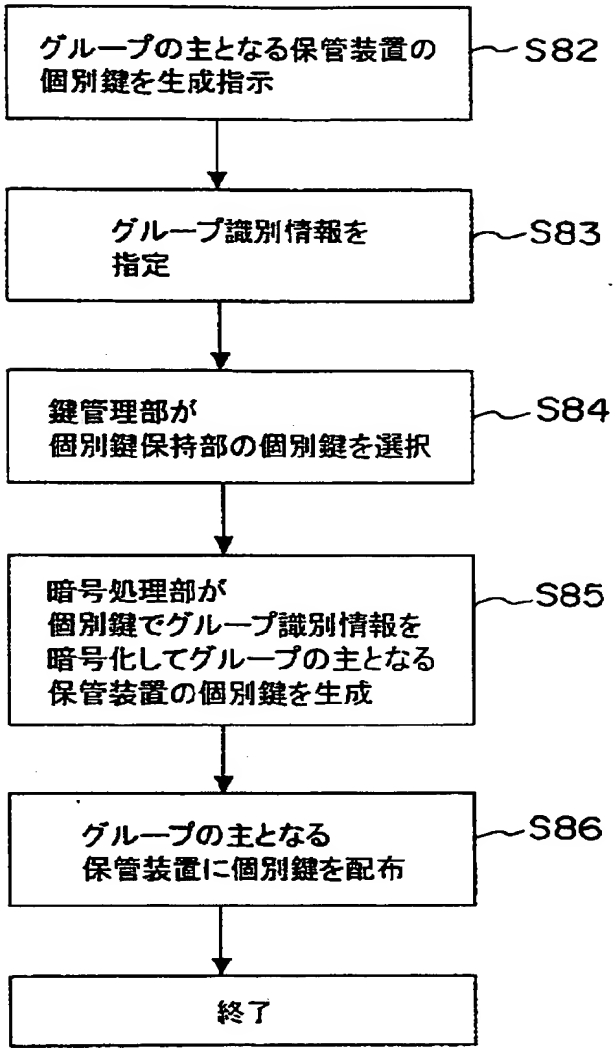
【図１３】

第２の実施形態における
グループ鍵生成処理のフローチャート



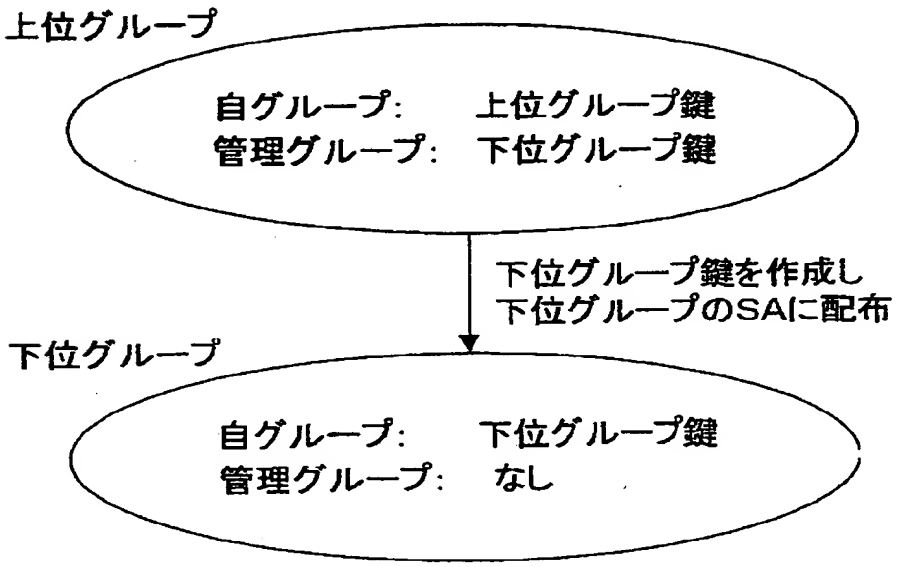
【図１４】

グループ管理保管装置による
グループマスタの個別鍵生成処理のフローチャート



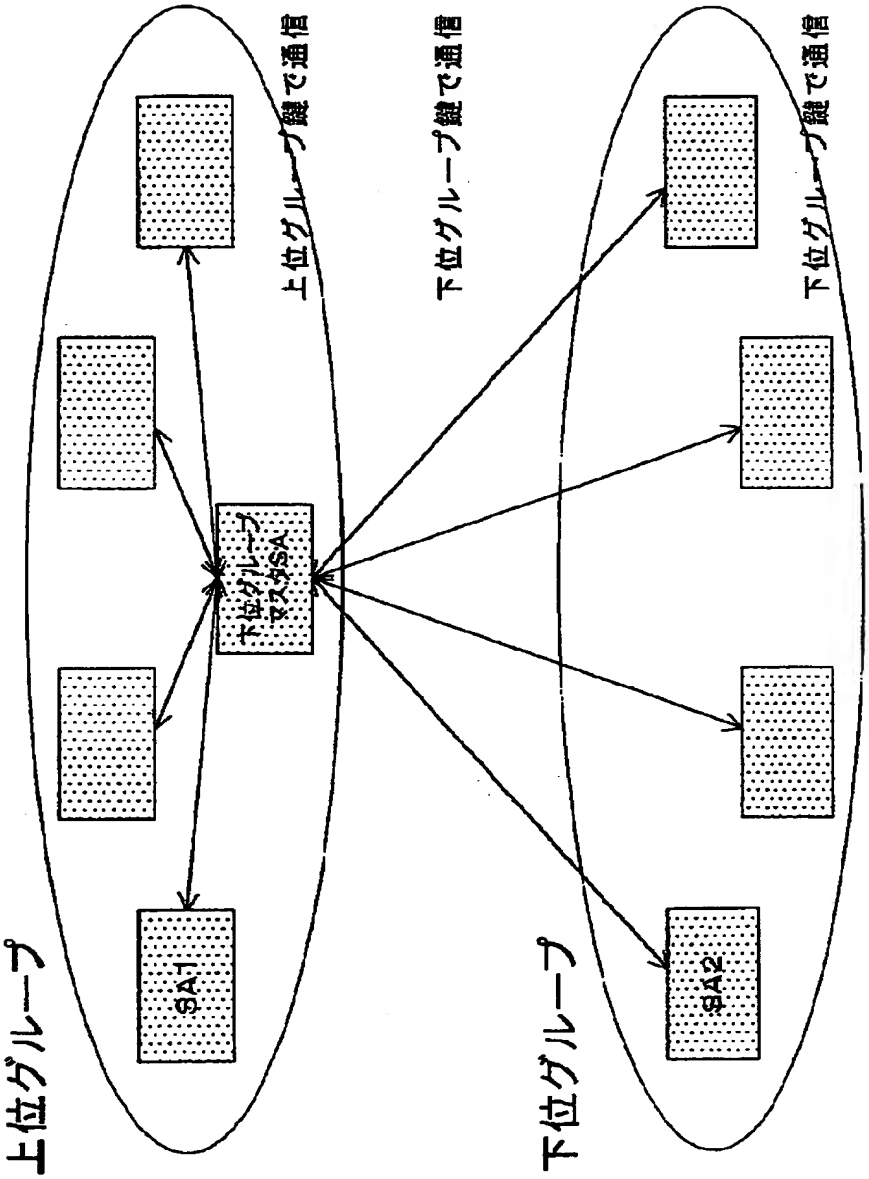
【図１５】

グループの階層化を説明する図



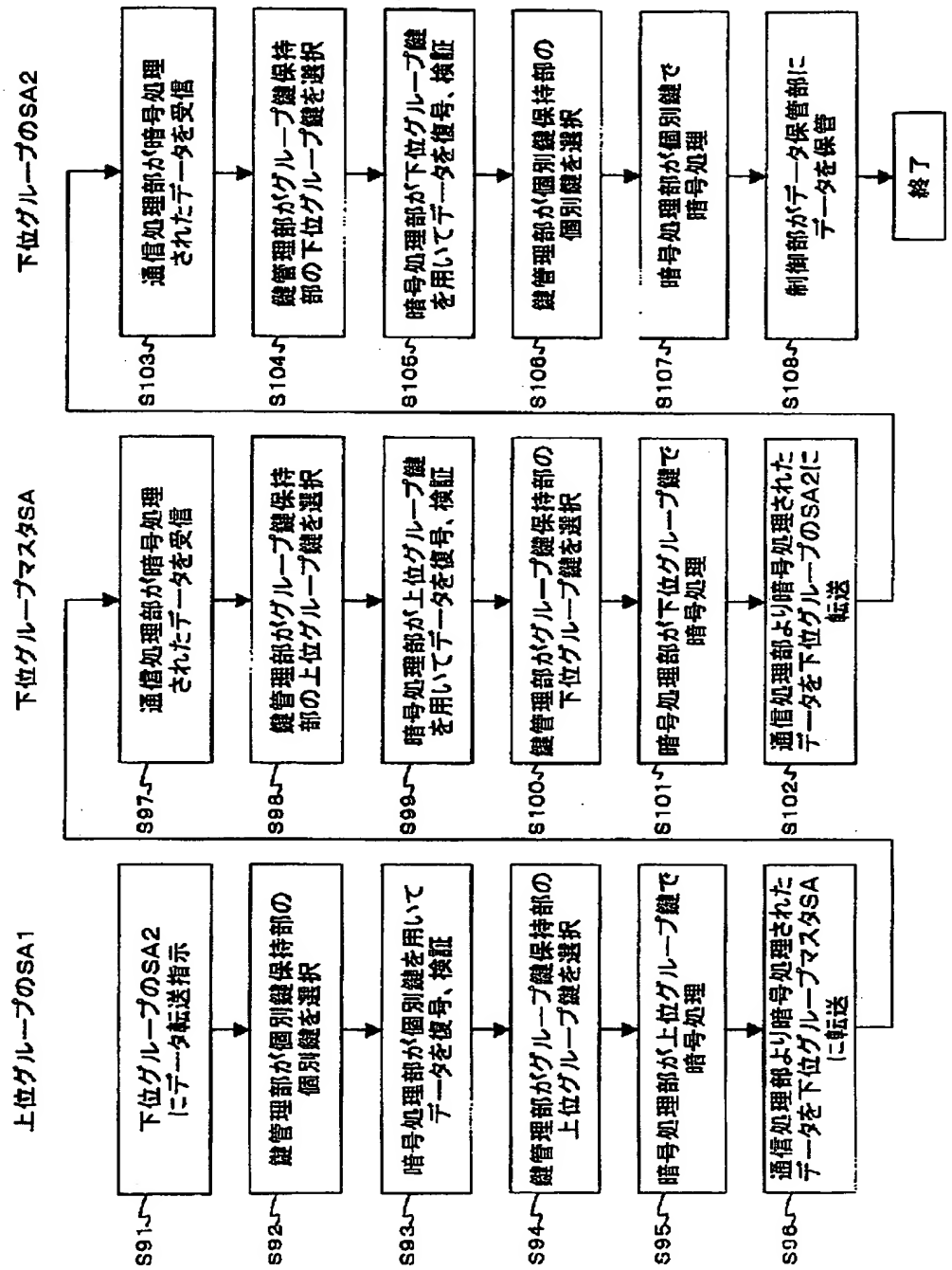
【図１６】

上位グループと下位グループの電子データ
保管装置相互間での通信を説明する図



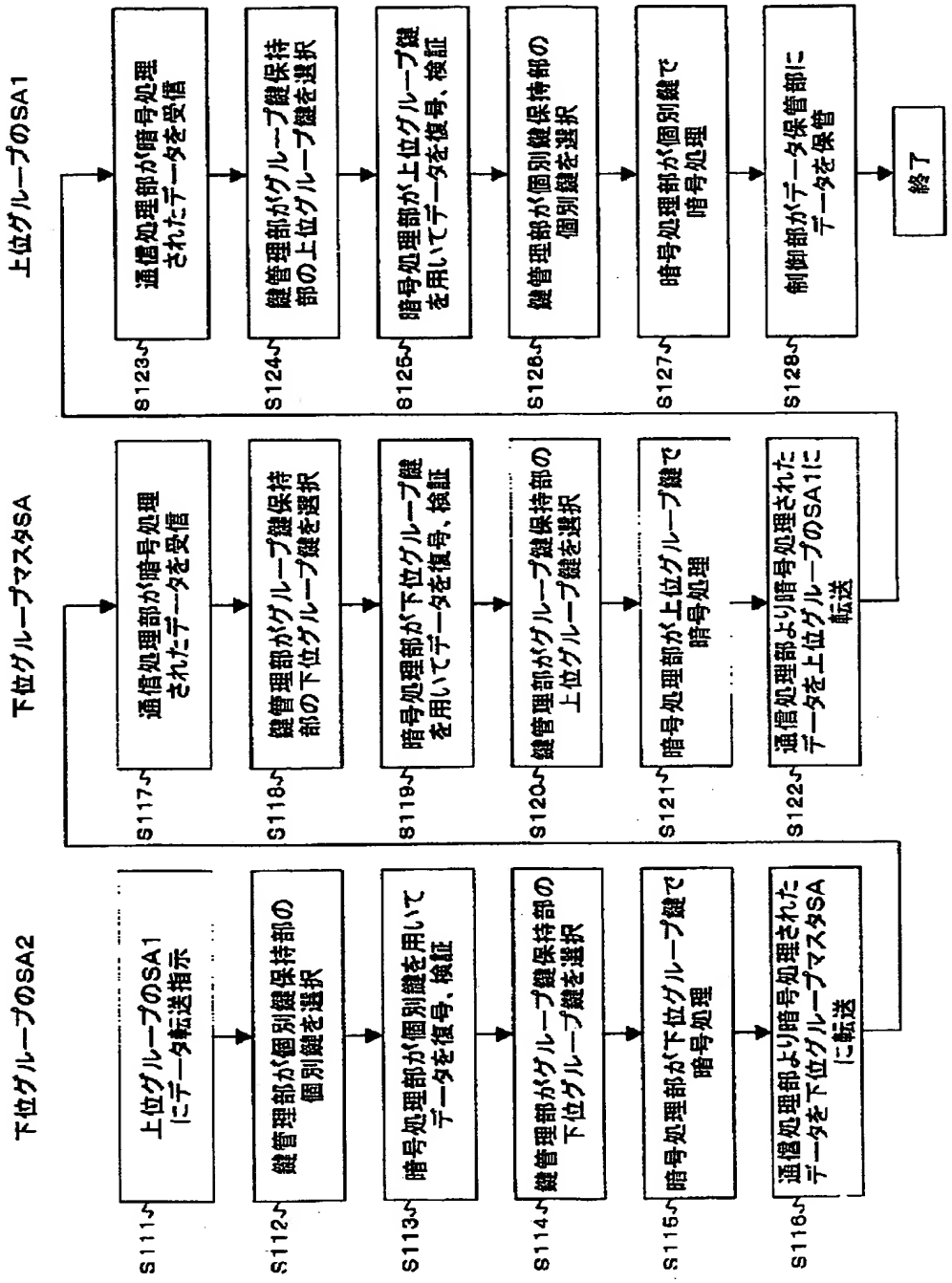
【図１７】

上位グループの保管装置から
下位グループの保管装置へのデータ送信処理のフローチャート



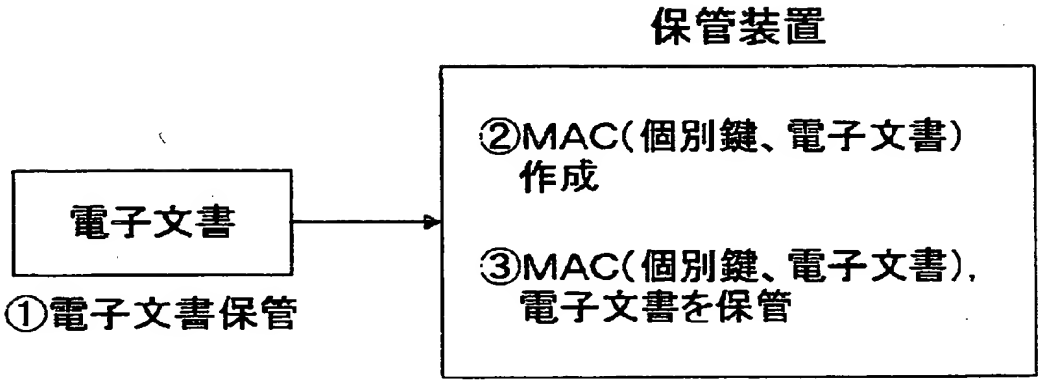
【図１８】

下位グループの保管装置から
上位グループの保管装置へのデータ送信処理のフローチャート



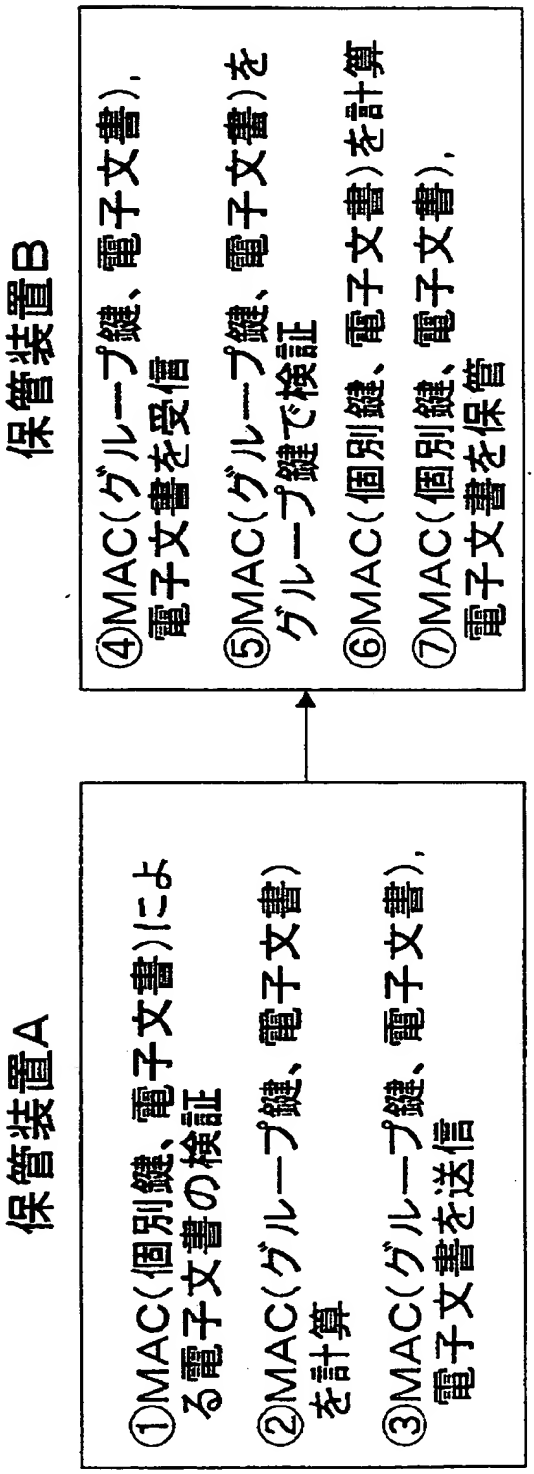
【図１９】

個別鍵を用いた電子文書保管の説明図



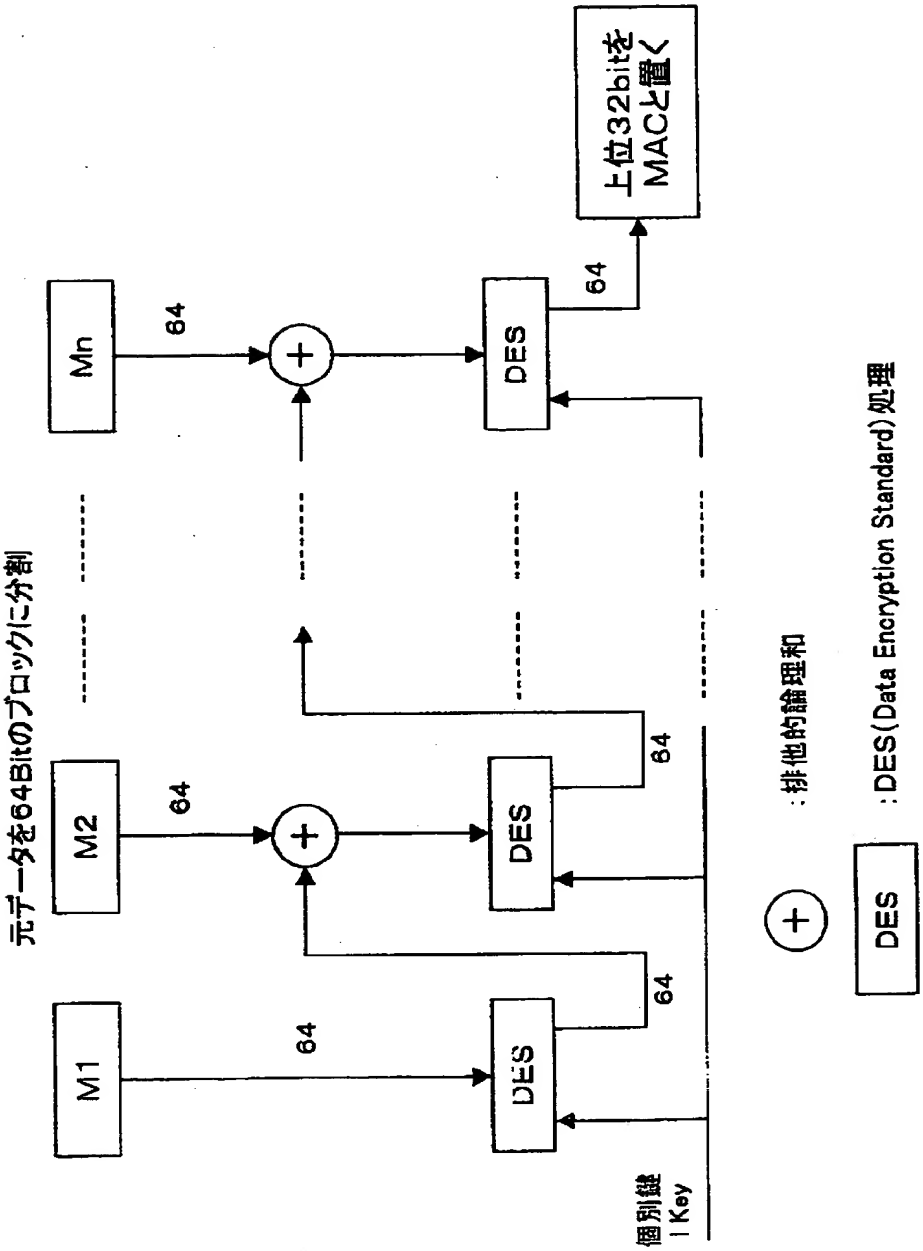
【図２０】

同一グループに属する２つの
保管装置の間でのデータ送受信を説明する図



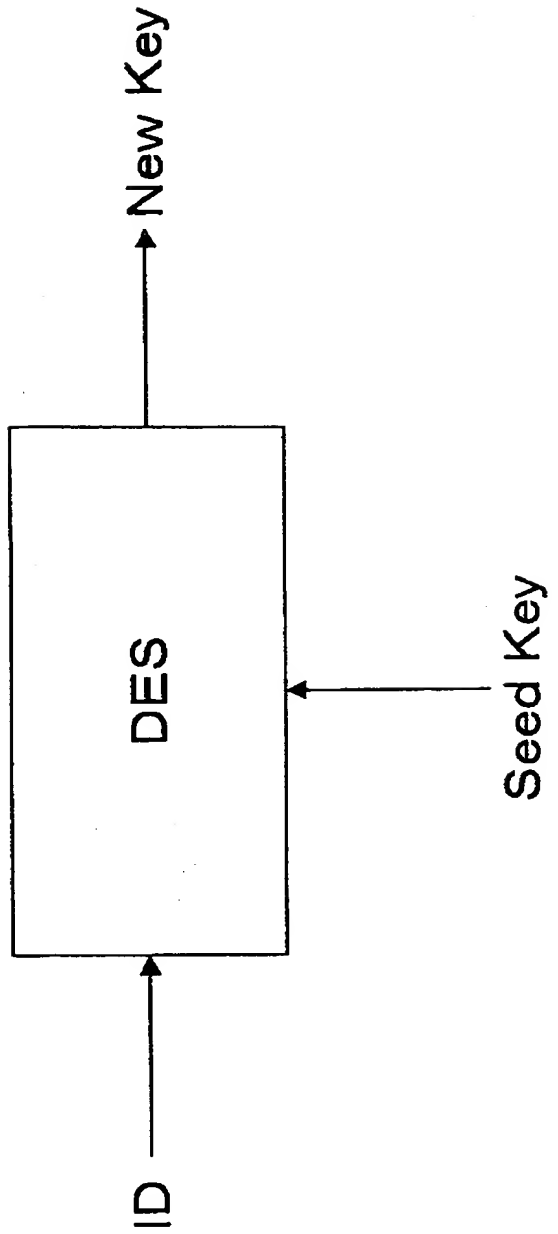
【図２１】

改ざん検出情報
MACの計算方法を説明する図



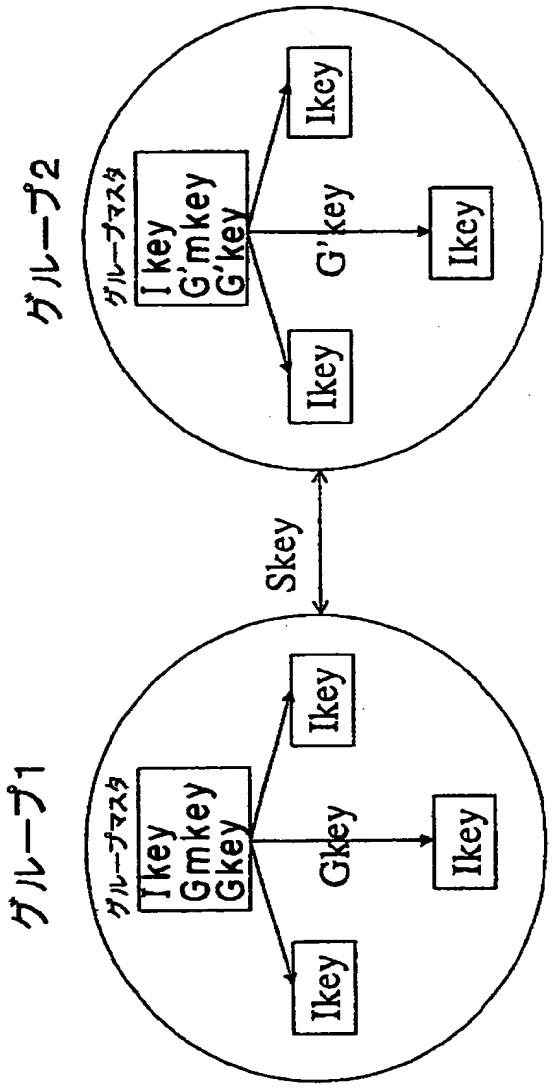
【図２２】

鍵の生成方法の説明図



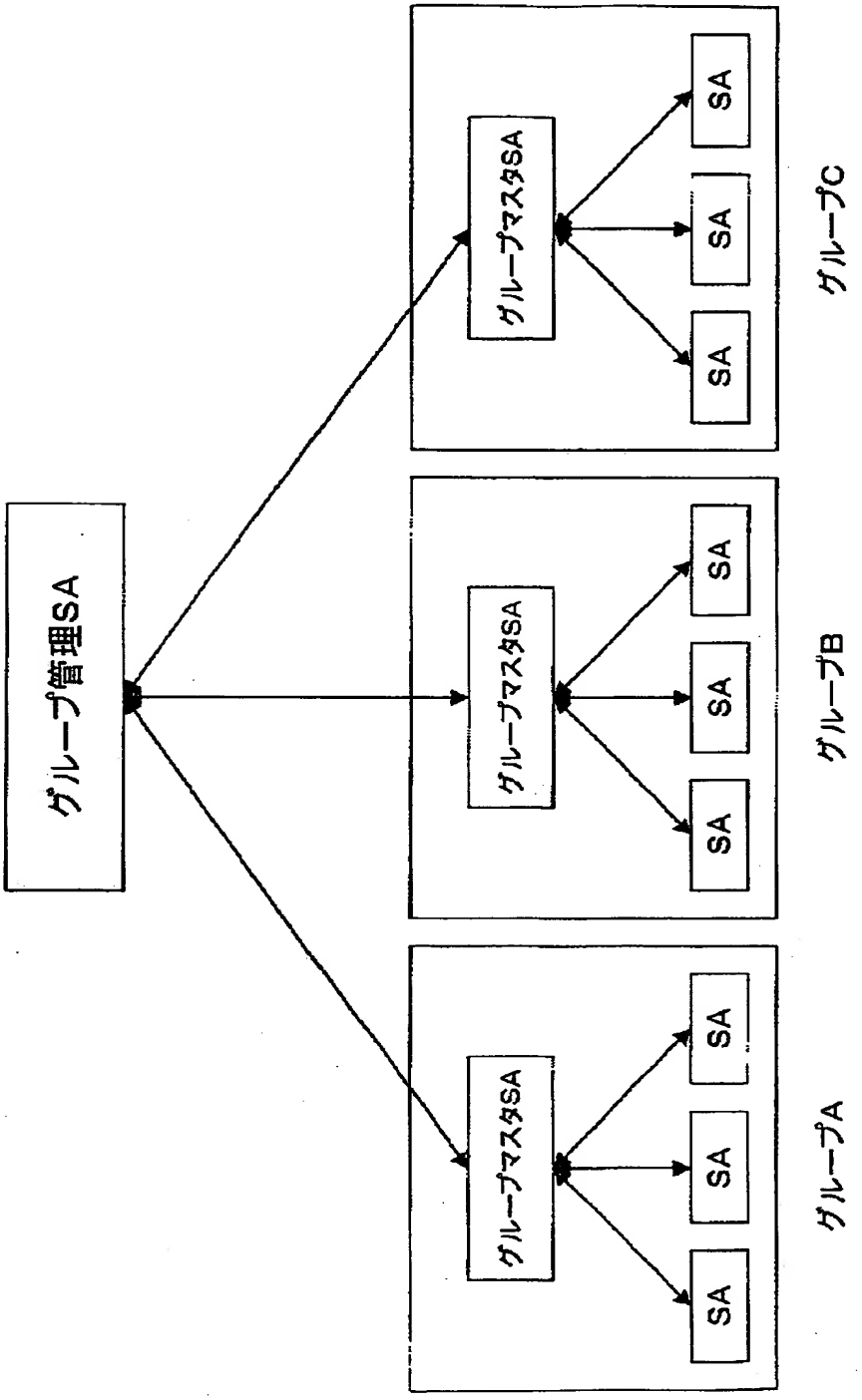
【図２３】

グループ鍵の生成とその配布を説明する図



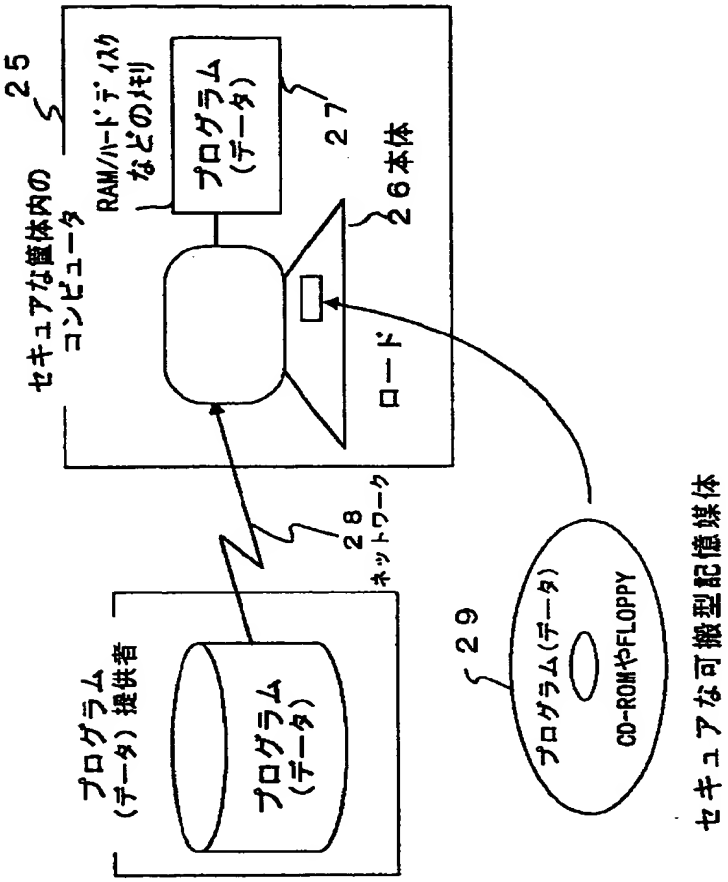
【図２４】

それぞれ複数のSAによって構成されるグループが複数存在する場合の、グループ管理SAによる全体管理方式の説明図



【図２５】

本発明の電子データ保管装置を実現するための
プログラムのコンピュータへのローディングを説明する図



【書類名】　　要約書

【要約】

【課題】　ローカルな環境とグローバルな環境にそれぞれ適合した共通鍵を用いて通信を行って環境に合った鍵管理を実現するとともに、電子データの安全性を確保する。

【解決手段】　自保管装置に固有の個別鍵と、他の保管装置との間で共通の共通鍵とを管理する手段２と、自装置内に保管する電子データに対しては個別鍵を用いて暗号処理を行い、他装置との間で送信、または受信する電子データに対しては共通鍵を用いて暗号処理、またはデータ検証を行う手段３とを備える。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
　［変更理由］　　住所変更
　　住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
　　氏　名　　富士通株式会社